UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Trabajo de titulación previa a la obtención del título de: INGENIERO E INGENIERA DE SISTEMAS

TEMA:

ANÁLISIS E IMPLEMENTACIÓN DE UN DIDS PARA GENERACIÓN DE FIRMAS DE COMPORTAMIENTOS ANÓMALOS EN LA RED DEL EDIFICIO MATRIZ DE LA EMPRESA ELÉCTRICA QUITO

AUTORES:

EDWIN SANTIAGO ACOSTA CORTEZ
JIMENA ALEJANDRA MUÑOZ VEGA

DIRECTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, mayo de 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN

Nosotros, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaramos que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad los autores.

Quito, abril 2015

_____	_____
Edwin Santiago Acosta Cortez	Jimena Alejandra Muñoz Vega
1715545818	1721979662

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación propone implementar una herramienta que ayudará a fortalecer la seguridad de la red del edificio matriz de la Empresa Eléctrica Quito, esta red tiene una topología tipo estrella extendida compuesta por aproximadamente 1500 dispositivos de comunicación los cuales generan gran cantidad de tráfico y pueden ser una brecha de seguridad para la red. Este Sistema de Detección de Intrusos Distribuido estará integrado por un servidor y sondas Pi, las sondas son las Raspberry Pi que básicamente son pequeños microprocomputadores.

Todo este sistema se montará sobre plataforma Linux con distribución Debian y Snort como motor principal del Sistema de Detección de Intrusos, cabe recalcar que tanto Snort como las distribuciones de Linux son OpenSource, brindando una gran ventaja económica para cualquier red sensada con IDS.

Las Sondas Pi se ubicarán en los puntos considerados más vulnerables, los cuales se comunicarán con el nodo central o servidor montado sobre Security Onion, el servidor recibirá eventos de las sondas procesados por Snort y los escribirá en la base de datos(Mysql) para presentar un análisis detallado en una interfaz gráfica llamada Snorby.

Esta interfaz reportará los eventos como alertas altas, medias y bajas en tiempos diarios, semanales, mensuales, como también detalles del tipo de protocolo, reglas usadas, direcciones y puertos de origen y destino de los cuales se generan las alertas. De esta manera se puede ayudar al administrador de la red con un análisis real de la situación actual de la red para que pueda prevenir futuras vulnerabilidades.

ABSTRACT

In This degree work, we proposed to implement a tool. It tool will help strengthen of network security of pricpal building of the Electric Enterprice Quito, It network has a extended star topology composed by aproximately 1500 communications devices the divices generate a lot of traffic and maybe a security network breach.The System Distributed Intrusion Detection will be composed by a server and sensors Pi, these sensors are Raspberry P1, essentially they're small microcomputers.

The System will be mounted on Linux plataform with Debian distribution and Snort as the main Intrusion Detection System, it should be emphasized both Snort and Linux will use the distribution is OpenSource, providing great economic advantage to whatever network IDS sensed.

The sensors pi will be located at the points considered most vulnerable, which will communicate with the central node or server mounted on Security Onion plataform, it server will receive events processed by Snort and it'll be written to the database (Mysql) to present a detailed analysis on a graphical interface called Snorby.

This interface will report events as high, medium and low alerts in daily, weekly, monthly times and also details the type of protocol used rules, addresses and source and destination ports which alerts are generated. This way you can help the network administrator with a real analysis of the current situation of the network so that you can prevent future vulnerabilities.

INTRODUCCIÓN

En la actualidad se puede apreciar que el número de usuarios que tienen acceso a Internet desde sus hogares y desde su área de trabajo que se hará referencia específicamente a usuarios que están dentro del edificio matriz de la Empresa Eléctrica Quito, ha crecido notablemente. Todo esto es debido al desarrollo inesperado en los últimos años de las tecnologías de transmisión de datos y el bajo costo de las mismas. Así como también se destaca el uso de Internet como medio de comunicación.

El gran desarrollo de la red de redes ha provocado que empresas con redes internas den acceso a su red a los usuarios desde sus hogares, otorgándoles permisos a las aplicaciones y datos confidenciales por medio del Internet hacia la red de la empresa a la que pertenecen.

Por esta razón diariamente es más frecuente enterarse de noticias que envuelven al Internet, como pueden ser problemas en el sistema informático o a su vez que algún virus o anomalías se propagan por la misma, ésta es la causa por la cual se ha producido un aumento considerable de los accesos no autorizados por parte de personas ajenas al sistema de información. Se ha comprobado que la mayoría de estos accesos se hacen por usuarios que quieren "probar" sus conocimientos en cuanto a informática.

No hay que dejar de lado que el acceso a sistemas con el propósito de obtener la información de forma incorrecta, está incrementando, la mayoría de estos accesos se realizan desde dentro de la misma red u organización que posee la información, llegando a ser estos ataques los más difíciles de descubrir y disuadir.

En el desarrollo de este proyecto de titulación se expondrá un Sistema de Detección de Intrusos Distribuido que monitoreará la red del edificio matriz de la Empresa Eléctrica Quito, con el fin de detectar accesos no autorizados y a su vez apoyar a los mecanismos de seguridad internos que actualmente dispone dicha organización, y de esta manera descubrir posibles brechas de seguridad que se puedan encontrar en esta red. Para explicar de mejor manera como se puede intentar acceder a una red que tenga las

vulnerabilidades suficientes ya sea dependiendo del sistema operativo o de los servicios que tenga activos en ella, el ataque procede de la siguiente manera:

- El intruso, realiza un escaneo de puertos y/o paquetes esperando encontrar algún servidor con fallo de seguridad, por lo general dentro de la organización este fallo suele ser conocido.
- El intruso usa un programa o exploit para crear una puerta de acceso al sistema.
- Una vez dentro del sistema el atacante instala una carpeta con nombre y comportamiento similares a los del sistema e inclusive muestra información sobre algunos estados del sistema.
- Una vez instalada la carpeta, el intruso compila algunas herramientas para escanear o atacar a otros equipos, usando a la maquina infectada como puente para llegar a otros dispositivos.

Con esta descripción de cómo puede producirse un ataque se concluye que el sistema a ser implementado , no solamente debe centrarse en los ataques de accesos no autorizados que se puedan producir, sino también en los escaneos de los puertos que el administrador de la red quiera controlar, de esta forma se logrará asegurar la información y brindar un sistema que apoye a la seguridad de esta red, al igual que se tendrá la ventaja de alertar al administrador de la red de las intrusiones al sistema interno que a la larga podrían ocasionar gran pérdida de información.

Con todo esto se comprueba que en la actualidad la información intangible es de alta prioridad, por lo cual se vuelve crítica, más aún si hablamos de la información de una red que conlleve datos sumamente importantes, en la cual la protección a la misma debe ser primordial. También hay que tener en cuenta que el incremento de usuarios en una red hace que la información sea más crítica debido a que se encuentra en un riesgo permanente, por los accesos autorizados y no autorizados que puedan hacer usuarios internos o externos de la red. Como puede ocurrir en el edificio matriz de la Empresa Eléctrica Quito debido a que se tiene alrededor de 1500 usuarios distribuidos en su edificio matriz. Por estas razones se debe tener presente que la información es vulnerable y hoy en

día se la puede proteger con una serie de mecanismos, los cuales pueden ser hardware y software dedicados.

A pesar de este tipo de prevenciones no todas las vulnerabilidades son conocidas, así como tampoco son conocidos los posibles ataques, por estos antecedentes la propuesta de esta tesis lleva a plantear una solución práctica y económica al alcance de cualquier administración de red que pretenda detectar intrusos en un forma proactiva, denominada Sistema de Detección de Intrusos Distribuido o como la llamaremos DIDS.

Los beneficiados con dicho proyecto de titulación son los usuarios y el administrador de la red del edificio matriz de la Empresa Eléctrica Quito. De forma más detallada se explicará el desarrollo de dicho proyecto de titulación, en los posteriores capítulos.

CAPÍTULO 1

ANÁLISIS DEL ESTADO DEL ARTE

1.1 Justificación de la problemática

La seguridad de una red es sumamente importante debido a que la información de las entidades gubernamentales y del campo energético es crítica, por lo cual debe ser protegida mediante algún mecanismo o sistema que brinde confidencialidad. En la actualidad la Empresa Eléctrica Quito cuenta con múltiples dispositivos de prevención hardware y software que brindan protección a información sensible de la red; pero debe reconocerse que hoy en día el advenimiento creciente de los APT (Amenaza Avanzada Persistente), requiere que las entidades revisen sus planes de respuesta a intrusiones e instalen sistemas que sean capaces de monitorear el tráfico en la red en busca de patrones anómalos. A raíz de esto se plantea una alternativa innovadora, rápida y económica; para fortalecer la seguridad de la red del edificio matriz de la EEQ, basada en hardware dedicado con Sondas Pi o técnicamente llamadas Rasberry Pi y con el uso de software libre como distribuciones de Linux, Snort, entre otros; con el fin de ayudar a mitigar posibles brechas de seguridad y con esto proteger de mejor manera la información de la red a ser estudiada que alberga más de 1500 usuarios distribuidos en los cinco pisos, por lo que es necesario la implementación de esta solución ya que el riesgo de intrusiones incrementa radicalmente.

Por esta justificación se ha planteado la implementación de un Sistema de Detección de Intrusos Distribuido con sondas Pi o Raspberry Pi, que será una solución muy útil, económica e innovadora que dará apoyo a la seguridad que actualmente disponen en el edificio matriz de la EEQ.

1.2 Objetivos

1.2.1 Objetivo general

- Analizar e implementar un DIDS para generación de firmas de comportamientos anómalos en la red del edificio matriz de la Empresa Eléctrica Quito.

1.2.2 Objetivos específicos

- Determinar las características, elementos y beneficios que proporciona la implementación de un Sistema de Detección de Intrusos Distribuido.
- Analizar el estado inicial de la red del edificio matriz de la EEQ, para determinar patrones de comportamientos normales y anormales a partir de los accesos que los usuarios realizan a los diferentes servicios de dicha red.
- Implementar el Sistema de Detección de Intrusos con sondas Pi, para la generación de firmas de los comportamientos anómalos, con el objetivo de mitigar ataques en los puntos críticos de la red del edificio matriz de la Empresa Eléctrica Quito.
- Generar un Script, que permita realizar la actualización de las reglas de Snort mensualmente.
- Analizar los resultados de las pruebas de la implementación del DIDS, para probar la eficiencia del sistema a implementar.

1.3 Descripción del DIDS a ser implementado

El producto que se espera implementar es un Sistema de Detección de Intrusos Distribuido (DIDS) basado en el motor de software libre de Snort conocido como IDS, un IDS o Sistema de Detección de Intrusos es una herramienta especializada que analiza e interpreta el tráfico de red para detectar actividades anormales o sospechosas y así reducir el riesgo de intrusión, el cual tiene una base de datos de firmas de ataques conocidos y puede comparar los patrones de tráfico o comportamiento de los datos que monitorea con los que tiene guardado en la base de datos y así detectar la posible intrusión. En este punto los IDS pueden emitir alarmas que informe a los administradores de la red del edificio matriz de la EEQ para que puedan tomar las precauciones del caso.

Existen tres clases de IDS que son:

- Sistema de Detección de Intrusos de Host (HIDS): orientados a examinar los datos en computadoras individuales.

- Sistema de Detección de Intrusos de Red (NIDS): tiende a examinar varios puntos de la red, es común encontrarlos de forma distribuida en la red.
- Sistema de Detección de Intrusos Distribuido (DIDS): éste es una mezcla de los dos anteriores. Este tipo de IDS permite detectar actividades sospechosas en base a los registros de su base de datos. Funcionan como sensores remotos y envían información pre procesada a una estación de administración central.

En este proyecto se usará sondas Pi o Raspberry Pi de tipo NIDS que monitorearán el tráfico de información en un segmento de red completo, buscando patrones de ataques en los puntos críticos de la red del edificio matriz de la EEQ, en las Sondas Pi se instalará SNORT que es una alternativa de Software libre para IDS, la sonda remota informará a una estación de administración centralizada llamada DIDS o Servidor. El servidor tendrá la base de datos de las firmas y ataques conocidos, de esta manera se podrá detectar las anomalías que afectan a dicha red y tomar decisiones de prevención proactiva, es decir, analiza un archivo y comparar su comportamiento con ciertos patrones que podrían indicar la presencia de una amenaza.

1.4 Primeros sistemas de detección de intrusos

En anteriores años a medida que crecía el uso de computadores, el análisis de los accesos por parte de los usuarios al sistema era tal que se volvía una tarea muy complicada de realizar. Las autoridades norteamericanas se dieron cuenta que el uso masivo de computadores requería de algún mecanismo que facilitara el análisis de seguridad de red.

La primera persona capaz de documentar la necesidad de un mecanismo que autorizara la revisión de los eventos de seguridad fue James P. Anderson que describió el concepto de "Monitor de Referencias" en un estudio encargado por las Fuerzas Aéreas de EEUU. Uno de los objetivos de este informe era la eliminación de información redundante en los registros de eventos. Anderson propuso un sistema de clasificación que distinguía entre ataques internos y externos, basados en si los usuarios tenían permiso de acceso o no al computador.

Los principales objetivos del mecanismo que presentó Anderson son:

- Proporcionar suficiente información para que los encargados de seguridad localizaran el problema, pero no para efectuar un ataque.
- Tener la capacidad de obtener datos de distintos recursos de sistemas.
- Para evitar ataques internos, debía detectar usos indebidos o fuera de lo normal por parte de los usuarios.

Anderson ideó un sistema para dar solución al problema de los intrusos, el cual distinguía entre el comportamiento normal o inusual de las cuentas basándose en patrones de uso, creados a partir del análisis de comportamientos de usuario.

El "Intrusion Detection Expert System" (IDES), fue creado en 1984 por Dorothy Denning y Peter Neumann, fue un modelo que definía un sistema de detección de intrusiones en tiempo real. Este proyecto, fundado entre otros por la Marina Estadounidense proponía un mensaje entre actividad anómala o uso indebido. Entendiendo por anormal, aquella actividad rara o inusual en un contexto estadístico. Usaba perfiles para describir principalmente a los usuarios del sistema, y reglas de actividad para definir las acciones de los eventos del mismo. Estos elementos permitían establecer mediante métodos estadísticos los patrones de comportamiento necesarios para detectar posibles anomalías. IDES era un sistema hibrido porque añadía un nivel de seguridad adicional mediante el uso de un sistema experto, basado en reglas de seguridad, que minimizaba los efectos de un intruso que intentara evitar el detector de anomalías.

Desde 1984 hasta 1985 un grupo de desarrollo en Sytek dirigió un proyecto denominado "Automated Audit Analysis", utilizaba información acumulada a nivel de interfaz de comandos "shell" de un sistema UNIX, para posteriormente compararlos con una base de datos. Estos datos se analizaban para demostrar que se podía detectar comportamientos fuera de lo normal.

Aquí se menciona algunos proyectos basados en el principio de IDES:

- *Discovery* fue un sistema creado para detectar e impedir problemas en la base de datos. La novedad de Discovery radicaba en que monitorizaba una aplicación, no un sistema

operativo. Utilizaba métodos estadísticos escritos en COBOL para detectar los posibles abusos. Su creador fue William Tener.

- El proyecto *Haystack*, del Centro de Soporte Criptográfico de las Fuerzas Amadas de los EEUU fue usado para ayudar a los oficiales a encontrar signos de ataques internos en los ordenadores principales de sus bases. Estas máquinas eran principalmente "mainframes" que manejaban información no clasificada pero confidencial. El sistema estaba escrito en C, ANSI y SQL. Examinaba los datos de forma periódica y recogía colas de eventos de igual manera. Utilizaba dos fases de análisis para detectar las posibles anomalías. El principal responsable del proyecto fue Steve Smaha.

- Otro proyecto importante fue el "*Multics Intrusion Detection and Alerting System" (MIDAS),* creado por el National Computer Security Center (NCSC). Al igual que IDES, MIDAS utilizaba un sistema hibrido en el que combinaba tanto la estadística de anomalías como reglas de seguridad de un sistema experto. MIDAS usaba un proceso de análisis progresivo compuesto por cuatro niveles de reglas. Además de estas reglas, también contaba con una base de datos que usaba para determinar signos de comportamiento atípico. Fue uno de los primeros sistemas de detección de intrusiones conectados a Internet. Fue publicado en la red en 1989. Dando como aporte el fortalecimiento de los mecanismos de autenticación de usuarios.

- El *"Network System Monitor" (NSM)* fue desarrollo en la Universidad de California para trabajar en una estación UNIX de Sun. Fue el primer sistema de detección de intrusiones que monitorizaba el tráfico de red, utilizando su propio tráfico como principal fuente de datos. Los anteriores sistemas utilizaban los eventos de sistema o registraban la digitación por teclado. El funcionamiento del NSM que muchos sistemas de detección de intrusiones de red utilizan hoy en día, se puede describir en estos pasos:
    - Ponía el dispositivo de red en modo promiscuo, de forma que monitorizara todo el tráfico que recibiera, incluido el que no iba dirigido al sistema.
    - Capturaba los paquetes de red.

- Identificaba el protocolo utilizado para poder extraer los datos necesarios (IP, ICMP, etc.).
- Utilizaba un enfoque basado en matrices para archivar y analizar las características de los datos, en busca de variaciones estadísticas que revelaran un comportamiento anómalo como de violaciones de reglas ya prestablecidas.

Una de las pruebas que se hicieron con el NSM monitorizó más de 111.000 conexiones, y detecto correctamente más de 300 posibles intrusiones. Los principales responsables del NSM fueron Karl Levitt, Todd Heberlein, y Biswanath Mukherjee de la Universidad de California.

1.4.1 Unión de sistemas de detección basados en máquina y basados en red

Durante los comienzos de la detección de intrusiones, la mayoría de los sistemas estaban pensados para monitorear dispositivos de red. A partir de los años 90, el rápido crecimiento de las redes de computadores hizo que surgieran nuevos modelos de intrusiones. El primer paso para la fusión de sistemas de detección basado en máquina y red fue el "Distributed Intrusion Detection System" (DIDS).

El DIDS fue el resultado del esfuerzo y el apoyo de grandes entidades como el Centro de Soporte Criptológico de las Fuerzas Aéreas de EEUU, el Laboratorio Nacional de Lawrence Livermore, la Universidad de California y los Laboratorios Haystack. Fue el primer sistema capaz de hacer que un grupo de seguridad pudiera monitorear las intrusiones de seguridad a través de las redes. El principal responsable de este proyecto fue Steve Smaha.

El objetivo inicial del DIDS era proporcionar medios que permitieran centralizar el control y publicación de resultados en un servidor central. El DIDS afronto diversos problemas. Los más importantes estaban relacionados con el hecho de tener que registrar eventos asociados a distintas máquinas a lo largo de la red. Un atacante suele aprovecharse de las redes para distribuir sus ataques realizando estos desde distintas computadoras. El DIDS fue el primer sistema capaz de relacionar los eventos que recibía para poder detectar una

posible intrusión. Además, reunían la información de forma que era posible hacer un seguimiento del posible intruso. (González Gómez, 2003, págs. 21-23).

1.5 Empresa Eléctrica Quito en Ecuador

1.5.1 ¿Qué es la EEQ?

La EEQ es una Institución que proporciona servicio público de electricidad, el área de concesión otorgada por el CONELEC a la Empresa Eléctrica Quito es de 14.971 Km2, correspondientes a los cantones Quito, Rumiñahui, Mejía, Pedro Vicente Maldonado, San Miguel de los Bancos, parte de Puerto Quito y Cayambe, en la provincia de Pichincha; así como Quijos y El Chaco en la provincia de Napo. La Empresa Eléctrica Quito, tiene la finalidad de proveer de servicio público de electricidad con calidad, eficiencia, solidaridad y responsabilidad, contribuyendo al desarrollo del sector eléctrico y la construcción del buen vivir. En la Figura 1 se describe el área de concesión que tiene la EEQ. (Empresa Eléctrica Quito, 2015).

Área de concesión de la Empresa Eléctrica Quito

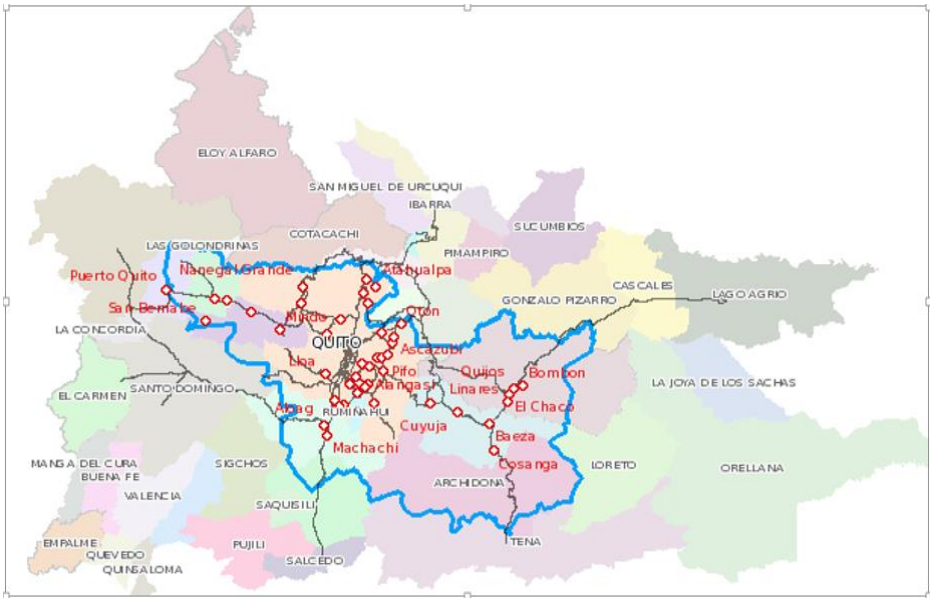


Figura 1 . Área de concesión de la EEQ.
Elaborado por: Santiago Acosta y Jimena Muñoz

Para cumplir con el compromiso y demás requisitos del cliente, la alta dirección aprobó el plan estratégico 2012 - 2015, basado en los siguientes ejes estratégicos:

- Consumidores satisfechos.
- Servicio público para todos.
- Eficiencia y diversificación energética.
- Responsabilidad social empresarial.
- Innovación tecnológica.
- Recurso humano capacitado y comprometido.

1.6 Estructura Organizacional de la Empresa Eléctrica Quito

El Directorio de la EEQ, en sesión del 2011-04-14, aprueba la nueva estructura organizacional a efectos de lograr mayor articulación y coordinación en la concesión de proyectos interinstitucionales y en general para propiciar un desarrollo local y nacional.

La nueva estructura organizacional obedece a una línea de mando desde la Gerencia General en correlación con las Gerencias a cargo de los procesos agregadores de valor: generación, distribución, comercialización y gestión de la energía desde la oferta y la demanda, así como también con la Gerencia Administrativa Financiera a cargo de los Procesos de Apoyo. (Empresa Eléctrica Quito, 2015).

En el siguiente nivel de mando se estructuran las unidades en función de su naturaleza y objetivos dentro de la Empresa Eléctrica Quito que se encuentra en proceso de reestructuración. En la Figura 2 se detalla de manera gráfica la organización de la Empresa Eléctrica Quito, determinando cada área con su respectivo responsable y la jerarquía que tiene cada uno de ellos.

Estructura organizacional de la EEQ

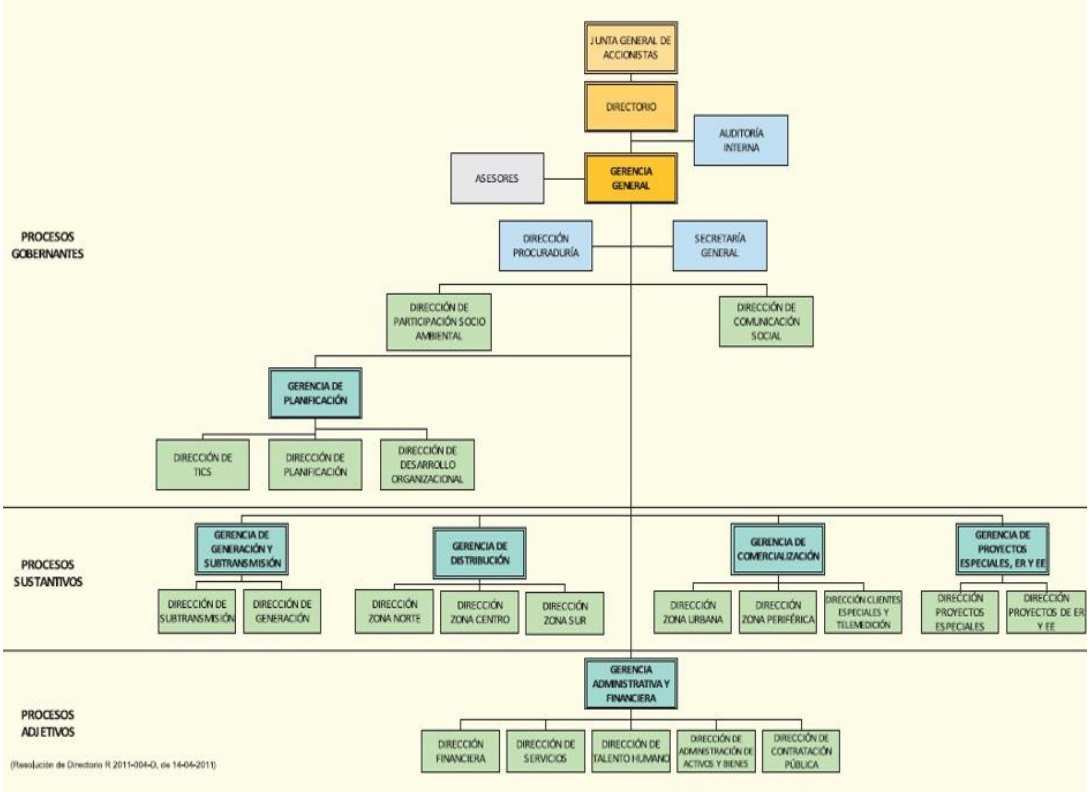


Figura 2. Estructura organizacional de la EEQ en sesión 2011.
Elaborado por: Santiago Acosta y Jimena Muñoz

CAPÍTULO 2

ANÁLISIS DEL ESTADO INICIAL DE LA RED DEL EDIFICIO MATRIZ DE LA EEQ

2.1 Estado inicial de la red de la EEQ

Actualmente la red de la EEQ tiene dos tipos de redes que son LAN y WAN. Las principales oficinas se encuentran estructuradas con red LAN y con estructura WAN en las subestaciones y centrales de generación. Los dispositivos de interconexión ubicados en el edificio matriz de la EEQ superan los 1500 dispositivos entre equipos como computadores de escritorio, portátiles, impresoras y nodos de comunicación.

La topología de la EEQ se basa en una topología estrella extendida ya que les da la facilidad de agregar dispositivos, prevenir daños o conflictos, permitiendo una excelente comunicación entre nodos de manera conveniente en la red.

Como información adicional se adjuntará en los anexos los diagramas de topología de fibra óptica, topología de Vlan's y de las subestaciones y centrales de generación de toda la red de la EEQ.

2.2 Análisis de la topología física de la red del edificio matriz de la EEQ

Una vez recolectada la información y los datos iniciales de la red, se obtiene el diagrama inicial de la topología física del el edificio matriz de EEQ está ubicado en Quito, en la Av. 10 de Agosto y Bartolomé de las Casas, conformado por una planta baja, mezzanine, 7 pisos y una terraza, cabe recalcar que el Data Center se encuentra en el primer piso y de ahí se puede encontrar los diferentes servidores que posee la EEQ.

- **Planta baja**

A continuación en la Tabla 1, se presenta la descripción de la topología física correspondiente a planta baja.

Tabla 1. *Topología física de la planta baja.*

P/P	Dispositivo en Piso		Interfaz	Enlace	Dispositivo Final Conectado	
	Descripción	Nombre			Descripción	Nombre
Baja	WS-C2960-24TT-L	CALL CENTER	GE		WS-C6509	Core las Casa

Nota. Descripción de la planta baja.
Elaborado por: Santiago Acosta y Jimena Muñoz

Todo esto se describe en la Figura 3 que se presenta a continuación.

Topología física de la planta baja

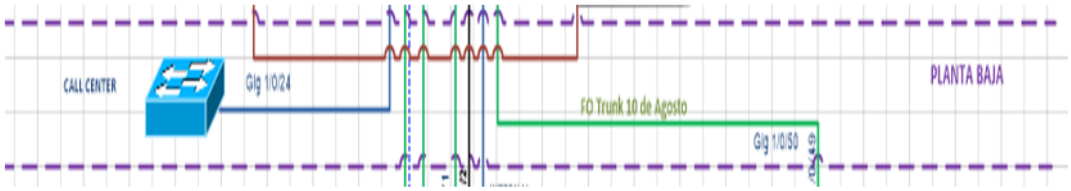


Figura 3. Topología física planta baja.
Elaborado por: Santiago Acosta y Jimena Muñoz

- **Mezzzanine**

En la Tabla 2, se describe la topología física del Mezzanine

Tabla 2. *Topología física de Mezzanine.*

P/P	Dispositivo en Piso		Interfaz	Enlace	Dispositivo Final Conectado	
	Descripción	Nombre			Descripción	Nombre
MEZZANINE	AP, AIR-LAP1131AG-A-K9	PIA	FE		WS-C2960S-24TS-S	PIA
	WS-C2960S-24TS-S	PIA	GE		WS-C6509	Core las Casa
				L2	Central Telefónica	TELEFONIA Las Casas

	Central Telefónica	TELEFONIA Las Casas	GE		WS-C6509	Core las Casa
	SW 3COM 16P	RECAUDACIÓN	GE		WS-C6509	Core las Casa
	WS-C2960-24TT-L	CONTROL BIENES	GE		WS-C6509	Core las Casa

Nota. Descripción del Mezzanine.
Elaborado por: Santiago Acosta y Jimena Muñoz

Para tener una mejor perspectiva la Figura 4, se presenta de la topología física de Mezzanine.

Topologia fisica del Mezzanine

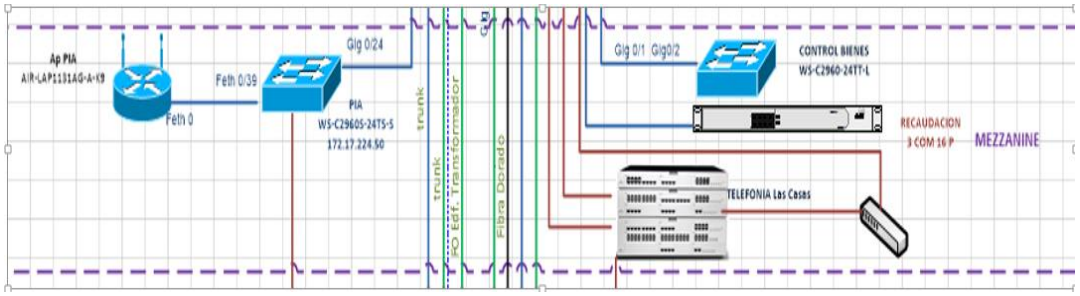


Figura 4. Topología física Mezzanine

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Primer piso**

En la Tabla 3, se explica la topología física del primer piso.

Tabla 3. *Topología física del primer piso*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
	Router	CNT 881 AGENCIAS	GE		WS-C6509	Core las Casa
	Router	TELCONET AGENCIAS	GE		WS-C6509	Core las Casa

PRIMER PISO	Router	EEQ_EXTRANET CNT 881	FE		Firewall	FIREWALL INTERNET
	Router	TELCONET_ EXTRANET	FE		Firewall	FIREWALL INTERNET
	Firewall	FIREWALL INTERNET	GE		WS-C6509	Core las Casa
	Servidor	Alcatel-OmniPCX Enterprise	GE		WS-C6509	Core las Casa
	WS-C3560G-24TS	SW_ENLACES DE RADIO	GE		Radios Enlaces	EDIF. TORRE ALBA
			GE		Radios Enlaces	MIRAVALLE
			GE		Radios Enlaces	EDIF. FORTUNE PLAZA
			GE		Radios Enlaces	CRUZ LOMA 1
			GE		Radios Enlaces	COLLALOMA
			GE			IMPRESORA GERENCIA
			GE			PATRICIA MENDOZA
			GE		WS-C6509	Core las Casa
	WS-C3560G-24TS	DIRECCIÓN TECNICA SUBESTACIONES	GE		Radios Enlaces	CRUZ LOMA CUMBAYA
			GE		Radios Enlaces	PERLABI
			GE		Radios Enlaces	PICHINCHA
			GE		WS-C6509	Core las Casa
	WS-C2960S-48TS-L	SOPORTE Y COMUNICACIONES	GE		WS-C6509	Core las Casa
				L2	AIR-LAP1131G-A-K9	REDES
	WS-C2960-24TT-L	SW_DESARROLLO	GE		WS-C6509	Core las Casa
	WS-C2960-24TT-L	HELP DESK	GE		WS-C6509	Core las Casa
	AIR-CT5508-K9	WIRELESS LAN CONTROLLER-EQQ	GE		WS-C6509	Core las Casa

Nota. Descripción del primer piso.
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 5, se representa lo que se ha descrito anteriormente del primer piso.

Topologia fisica del primer piso

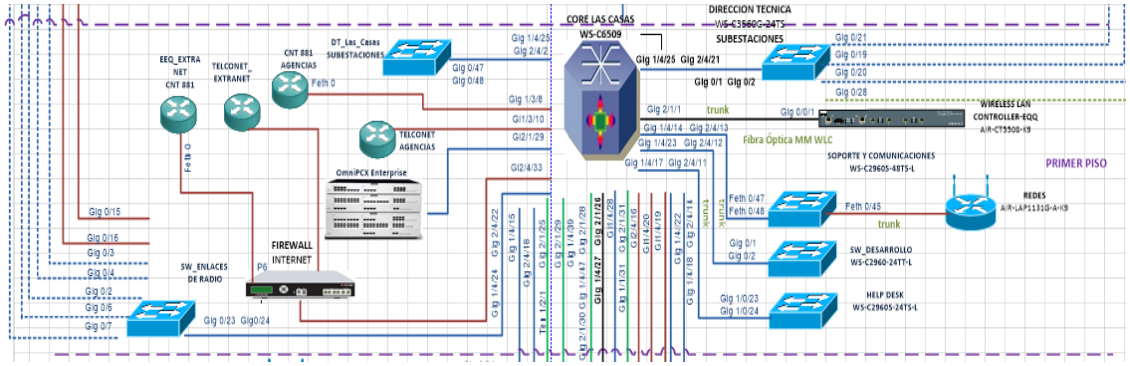


Figura 5. Topología física del primer piso

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Segundo piso**

La Tabla 4, se presenta la descripción de la topología física correspondiente al segundo piso.

Tabla 4. *Topología física del segundo piso*

Piso o Planta	Dispositivo en Piso		Interfaz	Enlace	Dispositivo Final Conectado	
	Descripción	Nombre			Descripción	Nombre
2p	WS-C2960-24TT-L	SW_ADQUISICIONES	GE		WS-C6509	Core las Casa
	WS-C2960-24TT-L	SW_TESORERIA	GE		WS-C6509	Core las Casa

Nota. Descripción del segundo piso.
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 6, se puede ver gráficamente la configuración de la topología física del segundo piso.

Topología fisica del segundo piso

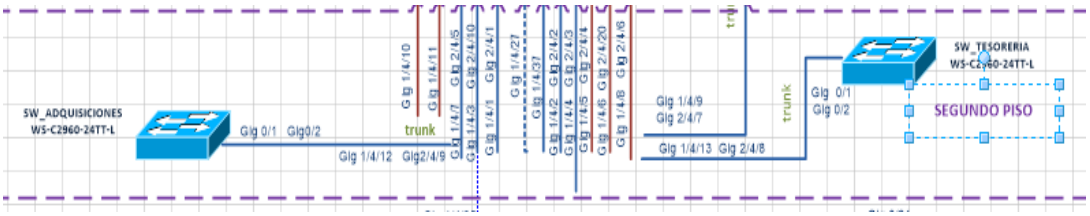


Figura 6. Topología física del segundo piso

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Tercer piso**

En la Tabla 5, se detalla la topología física del tercer piso.

Tabla 5. *Topología física tercer piso.*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
TERCER PISO	DLINK 8P	SELECCIÓN PERSONAL		L2	WS-C2960-24TT-L	SW_RRHH
	WS-C2960-24TT-L	SW_RRHH	GE		WS-C6509	Core las Casa
	AIR-LAP1131G-A-K9	AP_GERENCIA	GE		3COM 8P	SECRETARIA GERENCIA
	3COM 8P	SECRETARIA GERENCIA	GE		DLINK 8P	Sin Nombre
	DLINK 8P	Sin Nombre	GE		WS-C6509	Core las Casa
	3COM 8P	SW_ASESORIA	GE		WS-C6509	Core las Casa

Nota. Descripción del tercer piso.
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 7, se aprecia la topología física del tercer piso correspondiente al edificio matriz de la Empresa Eléctrica Quito.

Topología física del tercer piso

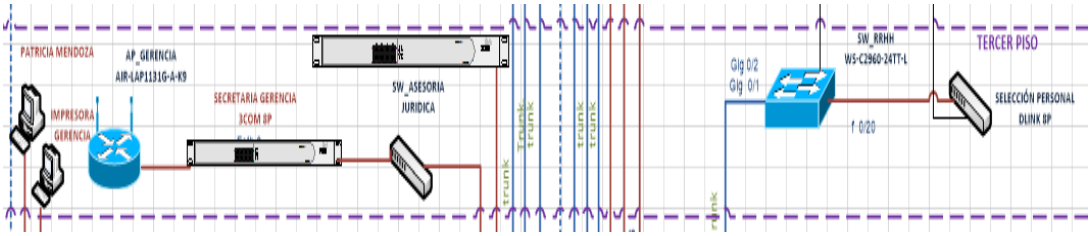


Figura 7. Topología física del tercer piso

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Cuarto piso**

A continuación en la Tabla 6, se presenta la descripción de la topología física propia del cuarto piso.

Tabla 6. *Topología física cuarto piso*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
CUARTO	AIR-LAP1131G-A-K9	AP_CONTABILIDAD	FE		WS-C2960-48TT-L	SW_CONTABILIDAD
	WS-C2960-48TT-L	SW_CONTABILIDAD	GE		WS-C6509	Core las Casa
	3COM 24P	DPTO PRESUPUESTO		L2_Acceso	DLINK 16P	DIRECCION FINANCIERA
				L2_Acceso	3COM 24P	DPTO PRESUPUESTO
			GE		WS-C6509	Core las Casa

Nota. Descripción del cuarto piso.

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 8, se personaliza lo que se ha descrito anteriormente correspondiente al cuarto piso.

Topología física del cuarto piso

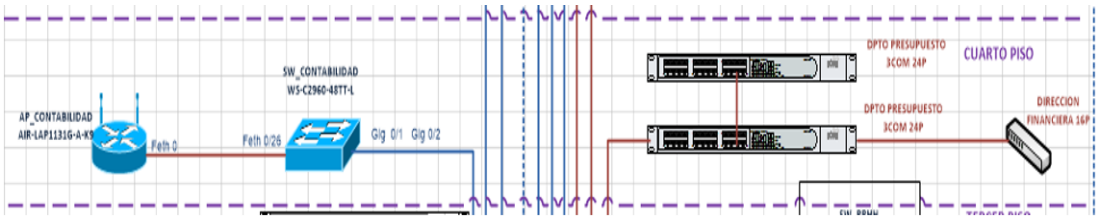


Figura 8. Topología física del cuarto piso

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Quinto piso**

En la Tabla 7, se puede estimar la descripción a topología física del quinto piso**.**

Tabla 7. *Topología física del quinto piso*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
QUINTO	3COM 16P	GESTION DE CALIDAD	FE		WS-C2960S-24TS-L	SW_INGCIVIL
	3COM 16P	GER. PLANIFICACION	GE		WS-C6509	Core las Casa
	3COM 16P	DPTO PLANIFICACIÓN Y GESTION	GE		WS-C6509	Core las Casa
				L2_Acceso	AIR-LAP1131G-A-K9	LC_Planificacion

Nota. Descripción del quinto piso.
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 9, se da la explicación la topología física del quinto piso.

Topología física del quinto piso

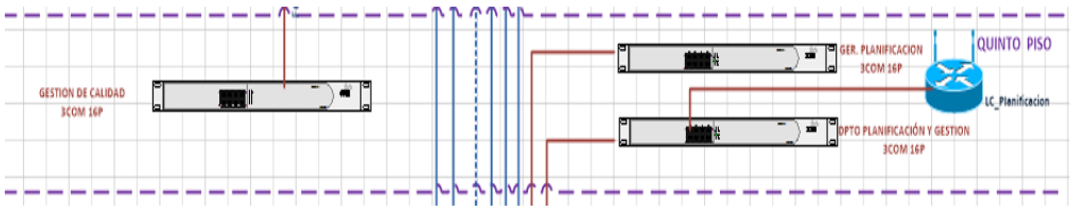


Figura 9. Topología física del quinto piso.

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Sexto piso**

En la Tabla 8, se detalla la topología física del sexto piso.

Tabla 8. *Topología física del sexto piso*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
SEXTO	AIR-LAP1131G-A-K9	AP_INGCIVIL	FE		WS-C2960S-24TS-L	SW_INGCIVIL
	CNET 16P	DPTO PROYECTOS	FE		WS-C2960S-24TS-L	SW_INGCIVIL
	WS-C2960S-24TS-L	SW_INGCIVIL	GE		WS-C6509	Core las Casa
			FE		3COM 16P	GESTION DE CALIDAD
	WS-C2960-24TT-L	SW_BIENES Y BODEGAS	GE		WS-C6509	Core las Casa
	3COM 16P	AUDITORIA	FE		WS-C2960-48TT-L	SW_DIR-GENERACION SITEMAS Y POTENCIA
			FE		AIR-LAP1131G-A-K9	AP_AUDITORIA

Nota. Descripción del sexto piso.

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 10, se explica la configuración en el piso sexto.

Topología física del sexto piso

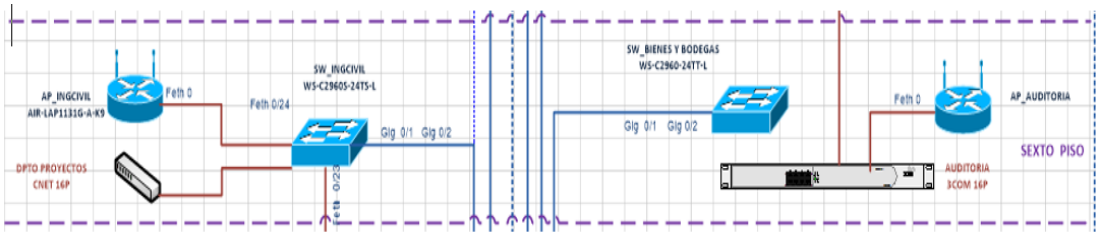


Figura 10. Topología Física del sexto piso

Elaborado por: Santiago Acosta y Jimena Muñoz

- **Séptimo piso**

En la Tabla 9, encontramos el cuadro de la topología física del séptimo piso.

Tabla 9. *Topología física del séptimo piso.*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
SÉPTIMO	WS-C2960-24TT-L	SW_DIV_GENERACION	GE		WS-C6509	Core las Casa
	WS-C2960-24TT-L	y SW_DIR-GENERACION SITEMAS Y POTENCIA	GE		WS-C6509	Core las Casa
			FE		AIR-LAP1131G-A-K9	AP_GENERACION
			FE		3COM 16P	AUDITORIA

Nota. Descripción del séptimo piso.
Elaborado por: Santiago Acosta y Jimena Muñoz

Se define la topología física del séptimo piso en la Figura 11.

Topología física del séptimo piso

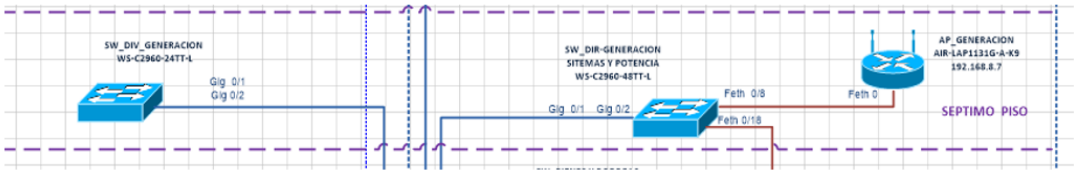


Figura 11. Topología física del séptimo piso.

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Tabla 10, se puede estimar la descripción a topología física de la terraza**.**

Tabla 10. *Topología física de la terraza*

Piso o Planta	**Dispositivo en Piso**		**Interfaz**	**Enlace**	**Dispositivo Final Conectado**	
	Descripción	**Nombre**			**Descripción**	**Nombre**
TERRAZA	WS-C2950-24	SW_TerrazaLC	GE		WS-C6509	Core las Casa
	Radios Enlaces	EDIF. TORRE ALBA	GE		WS-C3560G-24TS	SW_ENLACES DE RADIO
	Radios Enlaces	MIRAVALLE	GE		WS-C3560G-24TS	SW_ENLACES DE RADIO
	Radios Enlaces	EDIF. FORTUNE PLAZA	GE		WS-C3560G-24TS	SW_ENLACES DE RADIO
	Radios Enlaces	CRUZ LOMA 1	GE		WS-C3560G-24TS	SW_ENLACES DE RADIO
	Radios Enlaces	COLLALOMA	GE		WS-C3560G-24TS	SW_ENLACES DE RADIO
	Radios Enlaces	CRUZ LOMA CUMBAYA	GE		WS-C3560G-24TS	DIRECCIÓN TECNICA SUBESTACIONES
	Radios Enlaces	PERLABI	GE		WS-C3560G-24TS	DIRECCIÓN TECNICA

						SUBESTACIONES
	Radios Enlaces	PICHINCHA	GE		WS-C3560G-24TS	DIRECCIÓN TECNICA SUBESTACIONES
	Radios Enlaces	DORADO	GE		WS-C6509	Core las Casa

Nota. Descripción de la terraza.
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 12, se ve la configuración de la terraza.

Topología física de la terraza

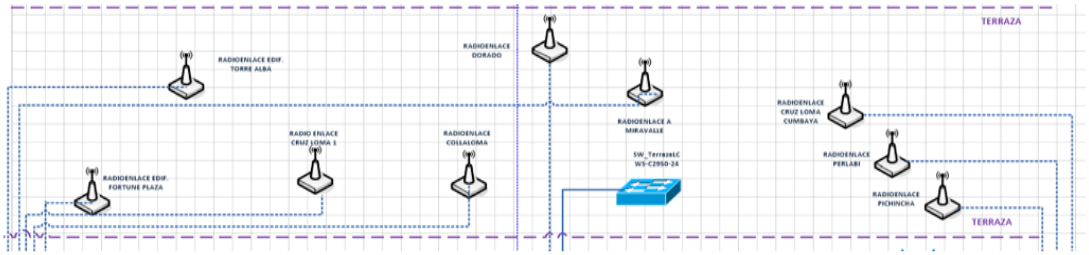


Figura 12. Topología física de la terraza.

Elaborado por: Santiago Acosta y Jimena Muñoz

2.3 Análisis de la topología lógica de la red del edificio matriz de la EEQ

En cuanto a lo referente a la topología lógica que tienen en el edificio matriz de la Empresa Eléctrica Quito a continuación se presenta el diagrama de dicha topología. En la Figura 13 se puede ver la configuración lógica del edificio matriz de la EEQ.

Diagrama de la topología lógica de la EEQ

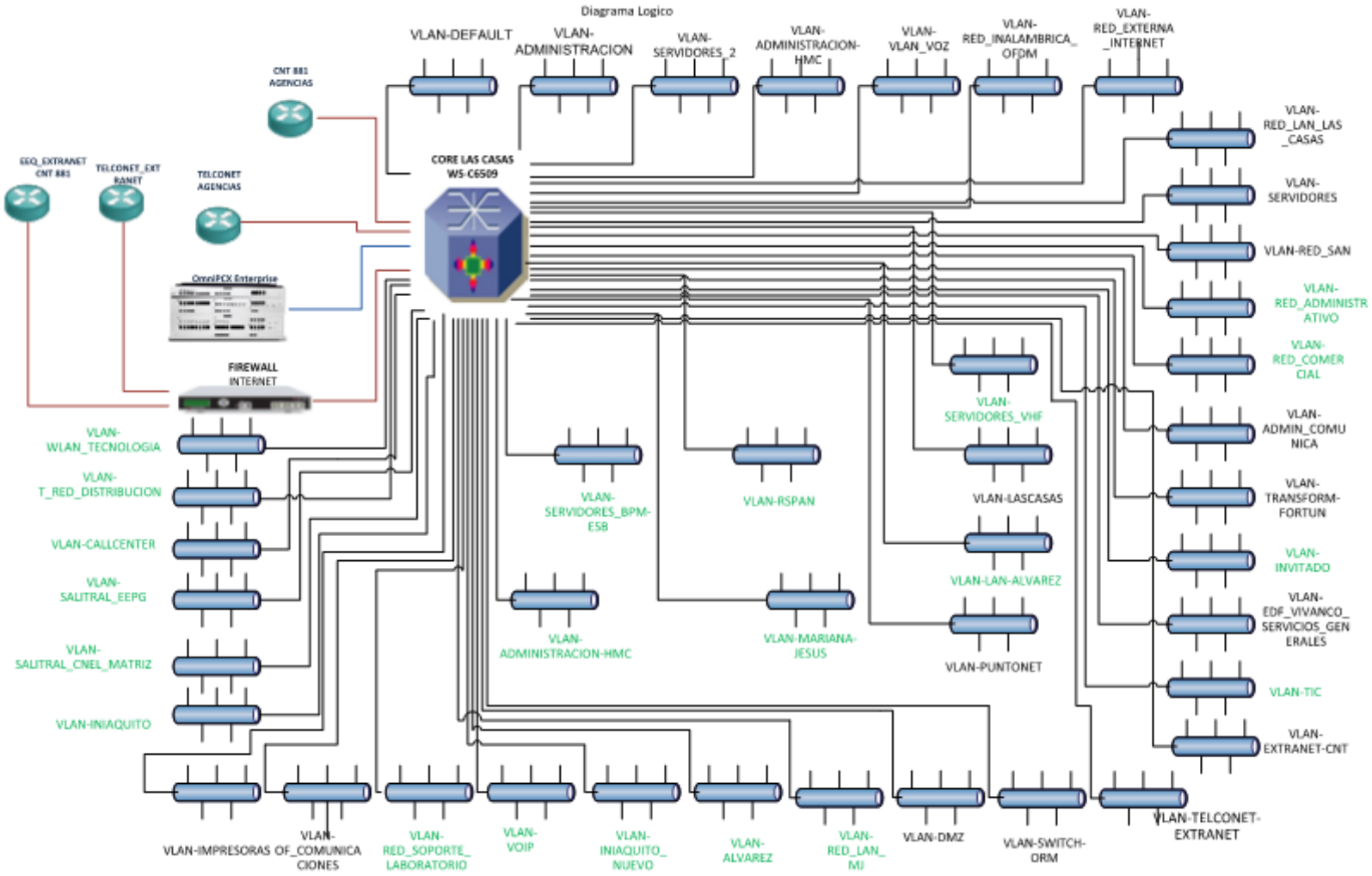


Figura 13. Diagrama de la topología lógica del edificio matriz de la EEQ.

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Tabla 11 se presenta el direccionamiento lógico de la configuración de las vlan's que tienen en el edificio matriz de la EEQ.

Tabla 11. *Direccionamiento lógico*

#	ID	Dirección	Interfaz
1	Default	132.147.161.20/22	Gi1/1/1, Gi1/1/2, Gi1/1/3, Gi1/1/5, Gi1/1/25, Gi1/1/27, Gi1/1/28, Gi1/1/29, Gi1/1/30, Gi1/3/3, Gi1/3/5, Gi1/3/6, Gi1/3/8, Gi1/3/10, Gi1/3/24, Gi2/3/20, Gi2/3/37, Gi2/3/38,Gi2/3/15, Gi2/3/16, Gi2/3/18, Gi2/3/11, Gi2/1/25, Gi2/1/27 Gi1/4/26, Gi1/4/35, Gi1/4/40, Gi2/3/39, Gi2/4/15, Gi2/4/23, Gi2/4/26, Gi2/4/40, Gi2/4/47, Gi2/4/48, Po1, Po4
2	ADMINISTRACION	172.17.224.1/23	Gi1/3/2, Gi2/4/31
3	SERVIDORES_2 (description RK7-D5-SRV_LICENCIAS_ARCGIS-ARCFM-VLAN3-172.17.226.11)	172.17.226.1/23	Gi1/3/29
4	Administracion-HMC		Active
5	VLAN_VOZ	172.16.44.1/23	Gi1/4/19, Gi1/4/20, Gi2/4/16, Gi2/4/17
6	RED_INALAMBRICA_OFDM		Active
8	RED_LAN_LAS_CASAS	172.16.2.1/24	Gi1/4/5, Gi1/4/11, Gi1/4/22, Gi2/4/4
9	SERVIDORESIMORESION	172.16.100.1/24	Gi1/3/13, Gi1/3/22, Gi1/3/23, Gi1/3/33, Gi1/3/34, Gi1/3/35, Gi1/3/37, Gi1/3/38, Gi1/3/39, Gi1/4/29, Gi1/4/30, Gi1/4/31, Gi1/4/32, Gi1/4/33, Gi1/4/34, Gi2/3/8, Gi2/3/9, Gi2/3/12, Gi2/3/33, Gi2/3/36, Gi2/3/44, Gi2/3/45, Gi2/3/46, Gi2/3/47,

			Gi2/3/48, Gi2/4/33, Po3, Po5, Po6, Po8
10	RED_SAN	192.168.30.13	Gi1/3/4, Gi2/3/19, Gi2/3/42, Po2, Po9, Po10
11	RED_ADMINISTRATIVO	172.17.231.1/24	Active
13	ADMIN_COMUNICA	172.16.102.1/23	Gi1/3/40, Gi1/3/41, Gi1/3/42, Gi1/3/43, Gi1/3/44, Gi1/3/45, Gi1/3/46, Gi1/3/47, Gi1/4/21, Gi1/4/38, Gi2/3/40, Gi2/3/43, Gi2/4/32
14	TRANSFORM-FORTUN	172.16.13.1/24	Gi1/3/14, Gi1/4/28
16	EDF_VIVANCO_SERVICIOS_GENERALES	172.16.16.1/24	Gi2/4/39
17	TIC	172.16.22.1/24	Active
18	EXTRANET-CNT	172.16.3.198	Gi1/3/7, Gi2/4/27
19	TELCONET-EXTRANET	132.147.160.91	Gi1/3/11, Gi2/4/29
21	DMZ		Gi2/3/17, Gi2/4/28
22	RED_LAN_MJ	172.16.36.1/23	Active
23	ALVAREZ	172.16.38.1/23	Active
25	INIAQUITO_NUEVO	172.16.240.1/24	Active
27	VOIP	172.16.242.1/24	Active
31	RED_SOPORTE_LABORATORIO	192.168.7.1/24	Active
32	OF_COMUNICACIONES	192.168.100.1/24	Gi1/4/10
33	IMPRESORAS	172.17.246.129/25	Active
34	INIAQUITO	172.16.34.1/24	Active
42	SALITRAL_EEPG		Active
43	CALLCENTER	172.17.247.193/26	Active
50	50 T_RED_DISTRIBUCION	172.17.229.1/24	Active
51	WLAN_TECNOLOGIA	172.17.230.1/25	Active
52	SERVIDORES_VHF	172.17.230.193/26	Active
53	LASCASAS	172.17.232.1/23	Gi1/4/6, Gi2/4/20
54	LAN-ALVAREZ	172.17.236.1/23	Active
55	PUNTONET		Gi1/3/12, Gi2/4/35
57	MARIANA-JESUS	172.17.234.1/23	Active
70	SERVIDORES_BPM-ESB	172.16.133.1/24	Active

Nota. Cuadro que contiene las vlan’s y direccionamiento lógico.
Elaborado por: Santiago Acosta y Jimena Muñoz

El direccionamiento establecido para la configuración de dicha red es: 172.16.1.0/24 - 172.16.102.0/24. Las subredes descritas anteriormente están siendo migradas a una subred la misma que está asignada con el direccionamiento: 172.17.224.0/19

Los servicios que actualmente se manejan en el edificio matriz Las Casas de la EEQ son:

- Intranet
- Internet
- Sistemas de bodegas
- Financiero
- Contabilidad
- Control bienes
- Telefonía
- Videoconferencia
- Chats por Gmail

2.4 Análisis de la red por medio de la interfaz Snorby

Partiendo del análisis inicial de la red a ser estudiada se verifica que la red está expuesta a una gran cantidad de amenazas debido al gran número de usuarios inexpertos que posee, para la obtención de información inicial acerca de estado de la red se procederá a usar una aplicación front-end idónea para este tipo de estudio, el cual se la conoce como Snorby. Esta herramienta permite hacer un análisis bastante amplio con lo que respecta a los eventos obtenidos después de un monitoreo de la red ya sea por enlaces o en general, presentando alertas de altas, medias y bajas severidades, en lo posterior se explicará de forma más detallada acerca de Snorby.

Con el reporte obtenido desde Snorby se procede a puntualizar y conocer el estado inicial en el que se encuentra dicha red, a continuación se describe brevemente las imágenes que Snorby reportó.

En la Figura 14, se tiene una visión rápida del conteo de eventos vs tiempo por sensor, en dicha imagen se reporta que el sensor de nombre SRCONION-eth0:1 abarca todo los eventos en un día, registrando un total de 8239.

Conteo de eventos vs tiempo

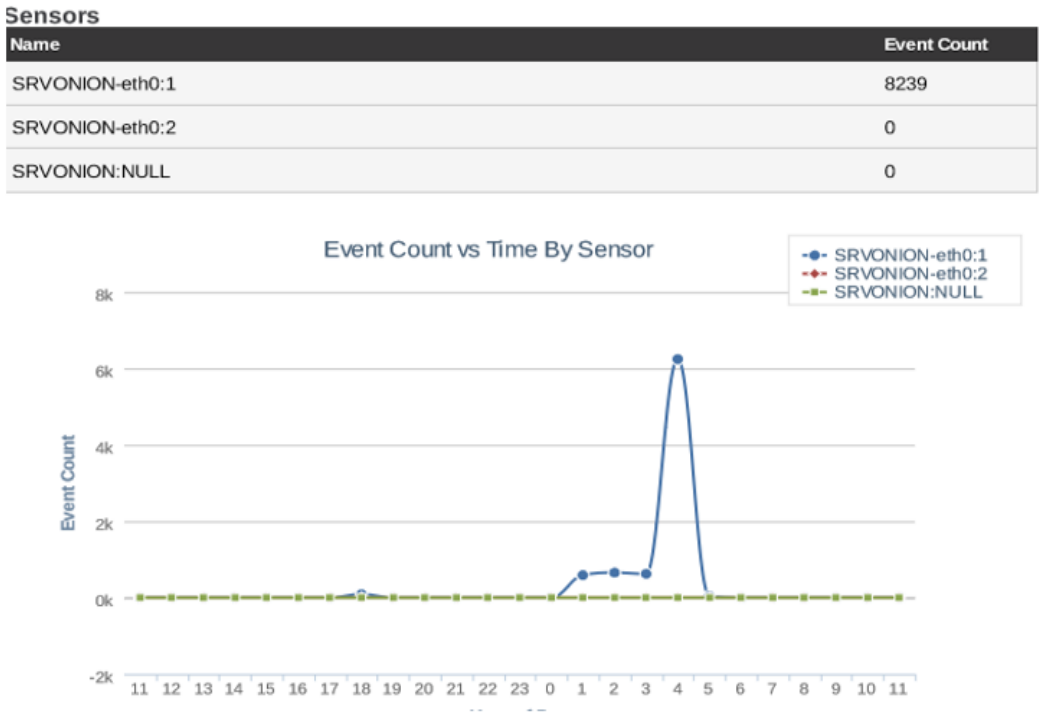


Figura 14. Conteo de eventos vs tiempo.
Elaborado por: Santiago Acosta y Jimena Muñoz.

En la Figura 15, se estima el conteo de alertas vs tiempo, reportando las alertas que son clasificadas como alertas altas de color rojo, alertas medias de color amarillo y alertas bajas de color verde, mediante el reporte de esta figura se puede apreciar que hay una alta exposición de amenazas graves seguidas de amenazas medias que en un punto pueden llegar a establecerse como alertas altas o críticas, esta es una de las razones por la que se propone este tema de titulación ya que esta herramienta podrá apoyar a la seguridad de esta red y a la toma de decisiones en mejoras de la misma por parte del administrador de red.

Conteo de alertas vs tiempo

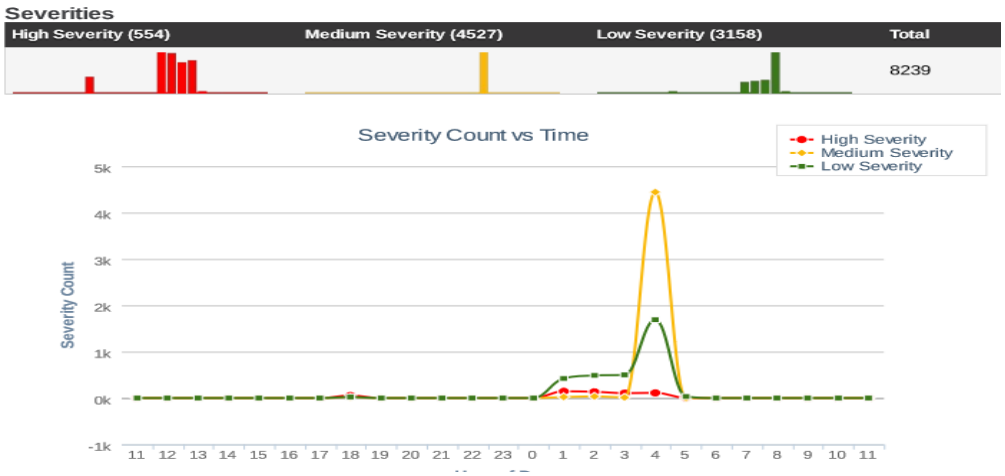


Figura 15. Conteo de alertas vs tiempo
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 16, se aprecia el conteo de protocolos vs tiempo, proporcionando como resultado los siguientes protocolos: protocolo TCP 7826, protocolo UDP 412 e ICMP 1 de un total de 8239 eventos generados. De igual manera se puede ver que la red del edificio matriz de la EEQ tiene un alto porcentaje de eventos de protocolos TCP los cuales pueden ser una brecha de seguridad en la transmisión de datos.

Conteo de protocolos vs tiempo

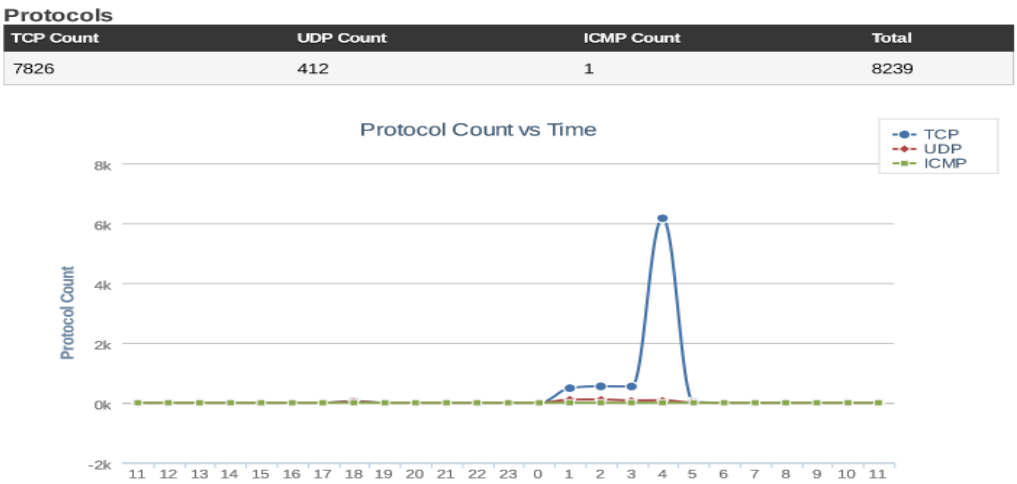


Figura 16. Conteo de protocolos vs tiempo
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 17, se presenta las "firmas" donde se especifica mediante un diagrama pastel las firmas que han generado un porcentaje de alertas, sobresaliendo la "ET INFO GENERIC SUSPICIOUS" que le corresponde el 54% de ataques genéricos sospechosos, entre otras firmas.

Estadisticas del reporte de las firmas de Snort

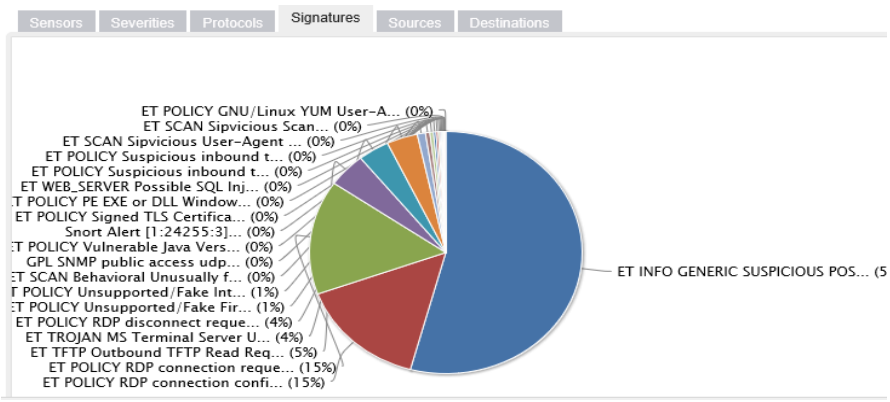


Figura 17. Estadística de reporte de las firmas
Elaborado por: Santiago Acosta y Jimena Muñoz

A continuación en la Figura 18 se muestra el Top 15 de las firmas, con el respectivo nombre, el porcentaje y el número de eventos. En esta figura se observa claramente que la red está generando un alto porcentaje de alertas dependiendo de la regla que detecta el ataque, con esto se puede verificar que es necesario el uso de una herramienta que apoye a la seguridad de dicha red.

Top 15 de la firmas reportadas por Snorby

Top 15 Signatures

Signature Name	Percentage	Event Count
ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Brows...	54.2%	4450
ET POLICY RDP connection confirm	15.25%	1252
ET POLICY RDP connection request	15.25%	1252
ET TFTP Outbound TFTP Read Request	4.55%	374
ET TROJAN MS Terminal Server User A Login, possible Morto inbound	3.71%	305
ET POLICY RDP disconnect request	3.68%	302
ET POLICY Unsupported/Fake FireFox Version 2.	0.96%	79
ET POLICY Unsupported/Fake Internet Explorer Version MSIE 5.	0.54%	44
ET SCAN Behavioral Unusually fast Terminal Server Traffic, Pot...	0.4%	33
GPL SNMP public access udp	0.3%	25
ET POLICY Vulnerable Java Version 1.7.x Detected	0.27%	22
Snort Alert [1:24255:3]	0.18%	15
ET POLICY Signed TLS Certificate with md5WithRSAEncryption	0.16%	13
ET POLICY PE EXE or DLL Windows file download	0.13%	11
ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	0.1%	8
ET POLICY Suspicious inbound to MSSQL port 1433	0.09%	7
ET POLICY Suspicious inbound to mySQL port 3306	0.07%	6
ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	0.06%	5
ET SCAN Sipvicious Scan	0.05%	4
ET POLICY GNU/Linux YUM User-Agent Outbound likely related to ...	0.05%	4

Figura 18. Top 15 de las firmas
Elaborado por: Santiago Acosta y Jimena Muñoz

La Figura 19, se encuentra la pestaña de Sources “fuentes”, en el que se puede observar las diferentes direcciones IP de origen que es de donde se genera el tráfico, en la figura un 54% es ocupado por la 172.17.232.42, este direccionamiento pertenece al enlace de LAS CASAS, es justificable que se tenga un porcentaje alto de eventos ya que es el origen de donde se monta el foco de monitoreo.

Cuadro estadístico de las direcciones ip de origen

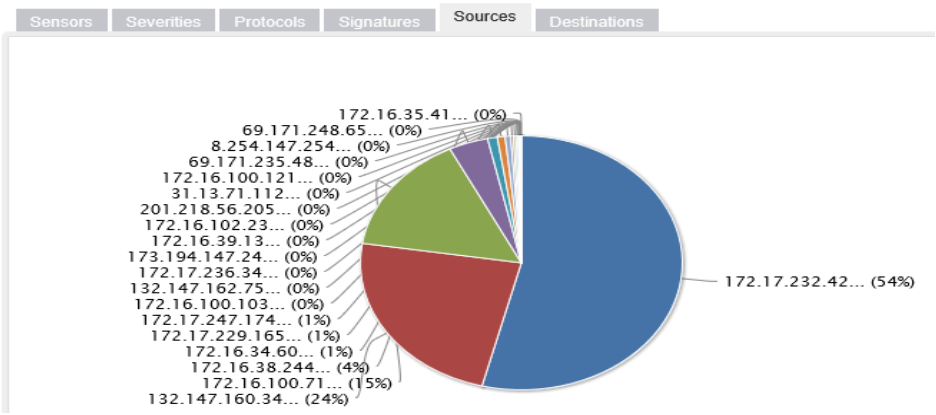


Figura 19. Fuentes o direcciones de origen IP
Elaborado por: Santiago Acosta y Jimena Muñoz

De una forma más detalla y precisa se muestra en la Figura 20 el top 10 de las direcciones de origen, en donde se describe las direcciones IP de origen con su porcentaje y número de eventos más destacados.

Cuadro estadístico de las direcciones de origen de los ataques

Top 10 Source Addresses

Source IP Address	Percentage	Event Count
172.17.232.42	53.93%	4430
132.147.160.34	23.52%	1932
172.16.100.71	15.24%	1252
172.16.38.244	3.94%	324
172.16.34.60	0.96%	79
172.17.229.165	0.78%	64
172.17.247.174	0.56%	46
172.16.100.103	0.27%	22
132.147.162.75	0.26%	21
172.17.236.34	0.19%	16

Figura 20. Top 10 de las direcciones de origen
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 21, se representa la gráfica de destinations “Destino”, en la cual presenta las diferentes direcciones IP de destino y la que ocupa un 54% es la dirección 162.250.2.2.

Diagrama estadístico de las direcciones de destino de los ataques

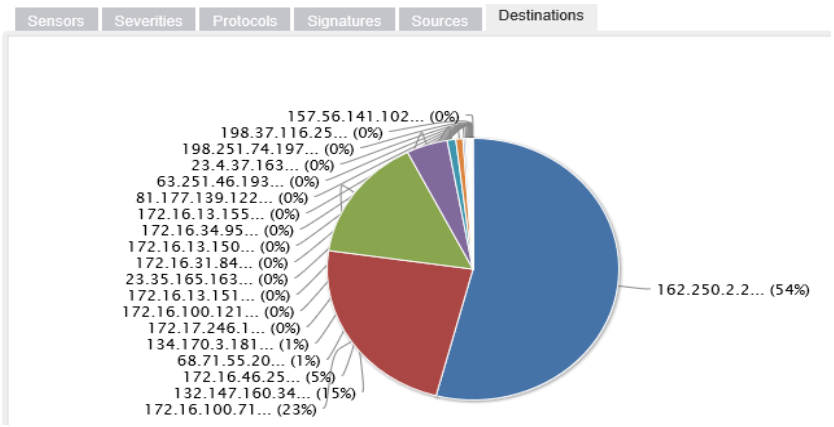


Figura 21. Direcciones de destino
Elaborado por: Santiago Acosta y Jimena Muñoz

En la siguiente Figura 22 se muestra el Top 10 de direcciones de destino, en donde se describe las direcciones de destino IP con cada uno de su porcentaje y la cantidad de eventos más destacados.

Cuadro estadístico de direcciones de destino de los ataques

Top 10 Destination Addresses

Destination IP Address	Percentage	Event Count
162.250.2.2	54.07%	4430
172.16.100.71	23.19%	1900
132.147.160.34	15.33%	1256
172.16.46.25	4.56%	374
68.71.55.20	0.96%	79
134.170.3.181	0.78%	64
172.17.246.1	0.26%	21
172.16.100.121	0.15%	12
172.16.13.151	0.12%	10
23.35.165.163	0.09%	7

Figura 22. Top 10 Direcciones de destino
Elaborado por: Santiago Acosta y Jimena Muñoz

Con el análisis del estado inicial de esta red obtenido del primer reporte adquirido de Snorby se puede detallar cada uno de los escenarios con sus posibles riesgos. A breves rasgos se puede apreciar que el tráfico que pasa por los enlaces de la red del edificio matriz de la EEQ es de gran afluencia, y por ende se puede tener más riesgos de intrusiones.

Algunos porcentajes de tráfico no solo se originan desde el edificio matriz, sino que se anexan al mismo enlaces de otros edificios cercanos que por las delimitaciones que se presentó en este proyecto de titulación no se los analizará, al igual que se puede ver que ciertos porcentajes se originan dentro de los enlaces o áreas que están en la red del edificio matriz, los que se destacan son: RED_DISTRIBUSION, CALLCENTER, SERVIDORIMPRESION. Así como hay origen se puede recalcar que los principales destinos que tienen interconexión los usuarios es a enlaces externos al edificio matriz e internos como CALLCENTER, LASCASAS, SERVIDORIMPRESION. Con el paso de estos datos se muestra que se activan algunas reglas que posteriormente se presentan como alertas en Snorby detectando incidentes troyanos, spyware, malware, backdoors, gusanos, entre otras según el protocolo y puerto que las conexiones hayan abierto y que las reglas detectaron.

Debido a la gran cantidad de datos que procesa dicha red, así como el número de usuarios que generan eventos que pueden asumirse como alertas altas, medias o bajas dependiendo de la actividad que realice y con lo analizado anteriormente se pone en evidencia que el uso de una herramienta de apoyo para la seguridad de red es necesaria, ya que esto puede generar una gran cantidad de brechas que pueden ser aprovechadas por intrusos que quieran dañar la integridad y confiabilidad de los datos.

CAPÍTULO 3

ANÁLISIS E IMPLEMENTACIÓN DEL DIDS

3.1 Diagrama de Diseño de la ubicación de las Sondas Pi.

Después de haber realizado el correspondiente análisis inicial de la red del edificio matriz de la EEQ, el diseño para la implementación del DIDS con sus respectivas Sondas Pi se muestra en la Figura 23 que es el diseño modificado con los enlaces principales que se encuentra en la Empresa mencionada. La ubicación física que se estima para las sondas pi se observa en la Tabla 12.

Tabla 12. *Ubicación física de las Sondas Pi*

Nombre Sonda	Enlace de ubicación
Sonda 1	Conectado desde Wireless LAN Controller – CORE las Casas, Vlan 13
Sonda 2	Conectado entre el switch Tesorería – CORE las Casas, Vlan 32

Nota. Ubicación física de las sondas en los enlaces a ser sensados
Elaborado por: Santiago Acosta y Jimena Muñoz

Las sondas Pi serán ubicadas en dichos enlaces de acuerdo con el diagrama modificado de la topología física (Figura 23), ya que son los enlaces que tienen mayor carga de tráfico y también donde están los departamentos de mayor importancia.

Diagrama de la topologia fisica modificado de la red de la EEQ

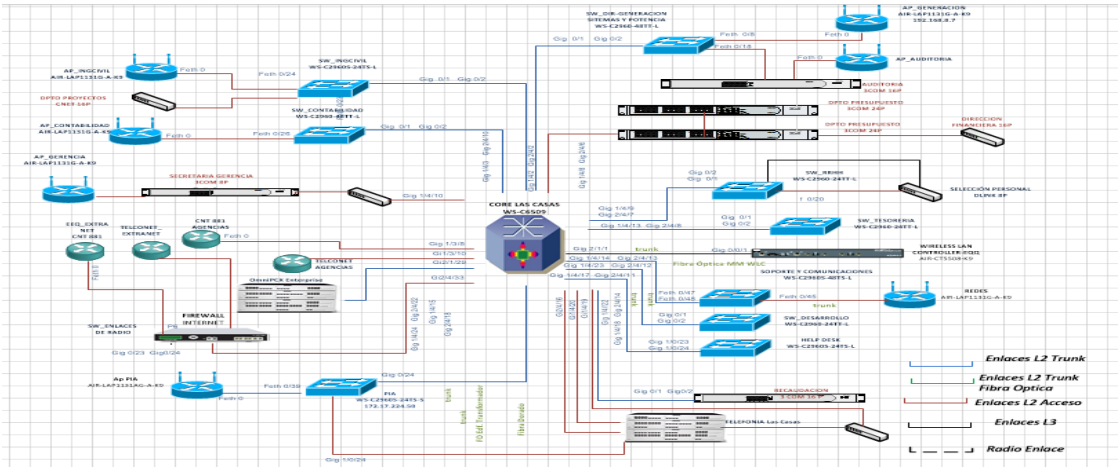


Figura 23. Diagrama modificado de la red de EEQ.
Elaborado por: Santiago Acosta y Jimena Muñoz

3.2 Descripción de las Raspberry Pi a usarse como sondas Pi

Los dispositivos que se van utilizar para analizar los enlaces de la red del edificio matriz de la EEQ que se mencionó en el punto anterior van a ser las sondas Raspberry PI modelo B, que por motivos de implementación en dicho proyecto de titulación se las denomino Sondas Pi. En la Figura 24 se muestra la Raspberry Pi o Sonda Pi.

Tarjeta Raspberry Pi modelo B

Figura 24. Raspberry Pi modelo B
Elaborado por: Santiago Acosta y Jimena Muñoz

La Sonda Pi es una microcomputadora con una arquitectura ARM con instrucciones de 32 bits, esta tarjeta requiere de menos transistores que los procesadores tradicionales, su costo es económico y el consumo de energía es mínimo, en sus inicios fue diseñada con el objetivo de enseñar a programar. Las Sondas Pi (Raspberry Pi) están diseñadas para funcionar con sistemas operativos basados en Linux. (Muñoz, 2014).

En lo que se refiere a los tipos de Raspberry Pi ofrecidas en el mercado se puede ver que hay tres modelos los cuales son:

- Modelo A
- Modelo B
- Modelo B+

3.2.1 Hardware de Raspberry Pi

La sonda Pi o Raspberry Pi es un dispositivo pequeño que muestra varias ventajas entre las cuales se destaca la posibilidad de mostrar video de alta definición o conectarse a redes, internet y administrar dispositivos de domótica. (Andrade, 2012).

Las sondas Pi están compuestas por varios puertos USB, un puerto Ethernet y salida HDMI, los cuales permiten conectar este dispositivo a otros como puede ser teclados, ratones y pantallas. Otras características que tiene son:

- System on Chip con procesador ARM
- Velocidad de procesamiento de 700 Mhz
- Procesador gráfico VideoCore IV
- 512 RAM
- Instalación de sistemas operativos a través de una tarjeta SD.

En cuanto a lo que se refiere del procesador ARM se dice que es una arquitectura RISC o conocida como Ordenador con Conjunto Reducido desarrollada por ARM Holdings. Actualmente ARM es conocida como Advanced RISC Machine. Ésta arquitectura es el conjunto de instrucciones de 32 bits , son utilizados en la actualidad para la electrónica de consumo tales como tabletas, teléfono inteligente, calculadoras y periféricos de computadores como discos duros y principalmente usada en Raspberry Pi o Sonda Pi (academia.edu, s.f., pág. 1).

En la Figura 25 que se muestra las partes que contiene una Raspberry Pi o Sonda Pi. A continuación se describe las especificaciones técnicas de la Raspberry Pi modelo B:

- CHIP: procesador de aplicaciones multimedia Full HD Broadcom BCM2835 SoC
- CPU: 700 MHz Procesador de aplicaciones de baja potencia ARM1176JZ-F
- GPU: dual Core VideoCore IV® Multimedia Co-Processor, conocida como unidad de procesamiento de gráficos, corre videos de full HD.
- RAM: 512 MB de SDRAM
- Ethernet: 10/100 Ethernet, conector RJ45.
- USB 2.0: conector USB dual, 2 puertos.

- Salida de vídeo: HDMI (rev 1.3 y 1.4)
- Tarjeta SD: esta es básicamente el disco duro de la sonda Pi, aquí se encontrar el sistema operático y carpetas de almacenamiento.
- Puerto GPIO: puerto de entradas y salidas de uso general, se puede conectar sensores y actuadores que permita interactuar con la Sonda Pi.

Representación del Hardware de la Raspberry Pi modelo B

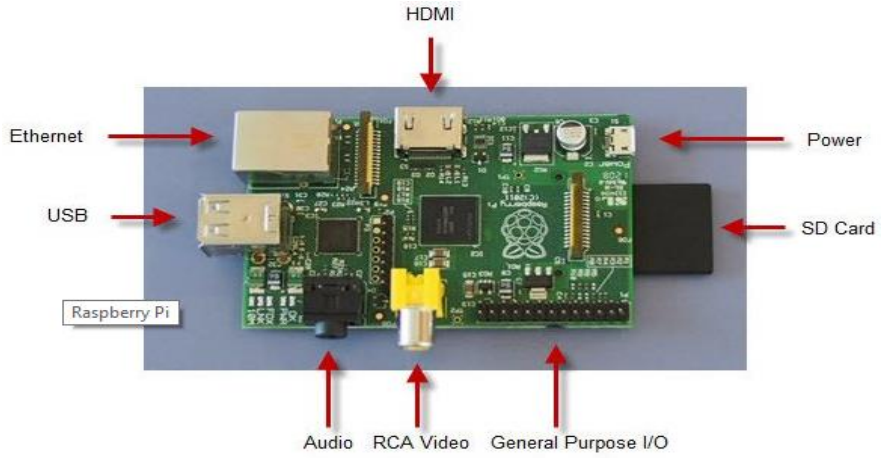


Figura 25. Hardware Raspberry Pi modelo B
Elaborado por: Santiago Acosta y Jimena Muñoz

3.2.2 Software de las Sondas Pi

La Sonda Pi o Raspberry Pi especialmente el modelo B, ha facilitado que la comunidad desarrolle distintos sistemas operativos principalmente en Linux con el objetivo de satisfacer distintas necesidades. Como se conoce el sistema operativo se carga desde una tarjeta SD, se puede tener varias distribuciones de Linux listas para ser cambiadas sin tener ninguna complicación. (Andrade, 2012).

El software nativo de la Raspberry Pi se denomina Raspbian que es una distribución de Linux basada en Debian, sin quitar que la Raspberry Pi puede soportar otras distribuciones que cumplan con la inter-operatividad con el hardware de la misma.

3.2.3 Comparativas de Sondas existentes en el mercado y Raspberry Pi

A continuación en la Tabla 13 se presentan comparativas entre diferentes placas vs la Raspberry Pi, en este cuadro se presentan las placas más conocidas en el mercado ya que en la actualidad se puede encontrar muchas placas con otras características.

Tabla 13. *Cuadro comparativo entre sondas Raspberry Pi y otras*

Nombre	**Raspberry Pi**	**Arduino Uno**	**BeagleBone**	**Intel Galileo**
Modelo	Modelo B	R3	Rev A5	Board
Precio	$60	$45	$89	$90
Tamaño	3.37”x2.125”	2.95”x2.10”	3.4”x2.1”	4.2”x2.8”
Procesador	ARM11	ATmega 328	ARM Cortex-AB	Intel® Quark™ SoC X1000
Velocidad del reloj	700MHz	16MHz	700MHz	400MHz
RAM	256MB	2KB	256MB	512KB
Flash	(SD Card)	32KB	4GB (microSD)	microSD
EEPROM		1KB		8Kb
Voltaje de entrada	5v	7-12 v	5v	5 -7v
Mini Energía	700mA (3.5W)	42mA (0.3W)	170mA (0.85W)	700mA(3.5W)
GPIO digital	8	14	66	12
Entrada Analógica	N/A	6 10-bit	7 12-bit	12
PWM		6	8	12
TWI / I2C	1	2	2	1
SPI	1	1	1	1
UART	1	1	5	1
Dev IDE	IDLE, Scratch, Squeak/Linux	Arduino Tool	Python, Scratch, squeak, Claud9?Linux	Microsoft Windows, Mac OS y Linux
Ethernet	10/100	N/A	10/100	10/100
Maestro USB	2 USB 2.0	N/A	1 USB 2.0	2 USB 2.0
Salida de vídeo	HDMI, Compuesto	N/A	N/A	N/A
salida de audio	HDMI, Análogo	N/A	Análogo	N/A

Nota. Cuadro de principales diferencias entre sondas Raspberry pi y otras.
Elaborado por: Santiago Acosta y Jimena Muñoz

3.2.4 Principales diferencias entre algunas Sondas y Raspberry Pi

3.2.4.1 Raspberry Pi VS. Arduino

Raspberry Pi, denominada también como SoC (System-on-Chip), se la presenta como una microcomputadora completamente funcional, el objetivo de esta placa es integrar todos

los elementos para ejecutar un sistema operativo, ya que contiene GPU, memoria, microprocesador, interfaces y periféricos. Capacidad para procesar tareas por sí misma.

En cambio Arduino es un microcontrolador que básicamente es parte de un computador , el cual no tiene la capacidad de realizar sus propios procesos como lo haría la Raspberry Pi, es decir no toma sus propias decisiones, pero si puede ser programado con aplicaciones en C.

3.2.4.2 Raspberry Pi Vs. BeagleBone

La diferencia entre la BeagleBone y Raspberry Pi es que no dispone de tantos puertos USB ni tiene la codificación de vídeo incorporado, haciendo que sea una desventaja para competir con Raspberry Pi en lo que es un sistema de entretenimiento.

3.2.4.3 Raspberry Pi Vs. Intel Galileo

La velocidad de procesamiento de Raspberry Pi es mucho más rápida en comparación con Intel Galileo. Raspberry Pi, trabaja muy bien en la manipulación de los medios de comunicación, tales como fotos o de vídeo, ya que tiene una unidad de procesamiento gráfico (GPU) y Galileo no la tiene. Y como gran desventaja es que el costo de Intel Galileo es casi el doble que el costo de Raspberry Pi.

3.3 Definición de Sistemas de detección de intrusos

Un sistema de detección de intrusos (IDS), se lo define como:

"Un elemento que escucha y analiza toda la información que circula por una red de datos e identifica posibles ataques. Cuando aparece un ataque, el sistema reaccionará informando al administrador mediante las alertas". (Giménez & Gómez, 2008, pág. 5)**.**

En una segunda definición se tiene**:**

La detección de intrusiones es el proceso de monitorizar redes empresariales o domésticas y sistemas en busca de violaciones de políticas de seguridad. (González Gómez, 2003, pág. 13).

"La clasificación más común de los IDS, se basa en tres características funcionales:

- **Fuentes de información:** corresponde al origen de los datos que serán usados para determinar si una intrusión se llevara a cabo.
- **Análisis:** concierne al método de detección se será utilizado. La información recogida en el paso anterior puede ser analizada mediante diferentes estrategias.
- **Respuestas:** una vez que se ha registrado alguna intrusión, los IDS pueden o bien responder de forma activa ante la misma o también registrar la detección y no realizar acción alguna." (Ortega, 2004, pág. 14)

Según las características funcionales de los IDS, se expone los siguientes tipos:

- **Sistema de Detección de Intrusos basados en maquina HIDS:** buscan patrones de anomalías conectados directamente a un computador o dispositivo de red.
- **Sistema de Detección de Intrusos basados en red NIDS**: los NIDS monitorizan, detectan y responden ante los datos generados dentro del tráfico de un enlace de la red local donde estén instalados.
- **Sistema de Detección de Intrusos Distribuido DIDS:** éste sistema es la combinación de los dos anteriores, que se comunican con un nodo central y detecta con mayor fiabilidad los ataques.

En este contexto resulta importante señalar que en el mercado existe un gran número de productos comerciales (NFR, Intruder Alert, NetProwler, RealSecure, eTrust, entre otros) y no comerciales (Snort, Dragon, Shadow, Intrudec, NetRanger, entre otros) de IDS, en este caso, se van a considerar los no comerciales, específicamente Snort por la compatibilidad con la plataforma Linux y principalmente por economía que es la principal ventaja que se pretende dar con esta solución de seguridad de redes.

3.4 Sistemas de detección de intrusos basados en máquina HIDS

Este tipo de detectores son capaces de hacer un análisis en tiempo real de los logs del computador o dispositivo que estén sensando para determinar actividades sospechosas. Al detectar algún cambio en los logs o ficheros de configuración del sistema, estos son comparados con los logs que tienen las políticas de seguridad o reglas de snort, en este análisis puede haber dos formas de realizar la comparación de los ficheros que son:

- En tiempo real cada vez que se realiza un cambio en los logs.
- Se realiza periódicamente por algún proceso que esté esperando en background.

Este tipo HIDS tiene la ventaja adicional de escuchar determinados puertos del sistema, y activar alarmas cada vez que detecten accesos no autorizados.

3.4.1 Ventajas de los IDS basados en máquina HIDS

- Los HIDS pueden monitorizar y detectar actividades específicas del sistema, como pueden ser modificaciones de ficheros o accesos a la computadora censada.
- Monitorización de los componente claves del sistema, es decir que pueden chequear la ejecución de los distintos programas del sistema, o librerías específicas.
- Se puede verificar los ataques, dado que este HIDS se basa en el análisis de los logs de la computadora analizada, así puede saber si el ataque inicializado tiene resultado o no.

3.4.2 Desventaja de IDS basados en máquina HIDS

- Los HIDS son más costosos de administrar, ya que son dispositivos individuales para cada computador de la red a ser monitorizada.
- Pueden ser deshabilitados por ciertos ataques de DoS.
- Usan los recursos del computador que están analizando, lo cual hace que el rendimiento de la misma base notablemente. (Mira Alfaro, 2001, pág. 19).

3.5 Sistemas de detección de intrusos basados en red NIDS

Los NIDS monitorizan la red, detectan y responden ante los datos generados, esto quiere decir que en vez de proteger un determinado host, proceden a recibir los datos de los enlaces de red local donde estén instalados. Mediante la utilización de dichos dispositivos de red ya configurados en modo promiscuo, capturarán todos los paquetes que pasen por él y procederá a almacenar la información de dichos paquetes en un repositorio para su posterior análisis. (Giménez & Gómez, 2008, pág. 15). Hay que tener en cuenta que se debe aplicar un filtro a este tráfico para determinar cuáles de los paquetes serán tomados en cuenta y cuáles serán descartados para el análisis correspondiente. Por lo cual los NIDS poseer un módulo de reconocimiento de paquetes que aplican tres métodos que son (Coll Almela, 2001, pág. 18):

- Marcas típicas de ataque
- Reconocimiento de patrones en el contenido de los paquetes
- Detección de acciones anómalas.

A continuación en la Figura 26 se representa de manera gráfica como funcionaria una NIDS para que se pueda comprender de mejor manera

Sistema de detección de intrusos basado en res NIDS

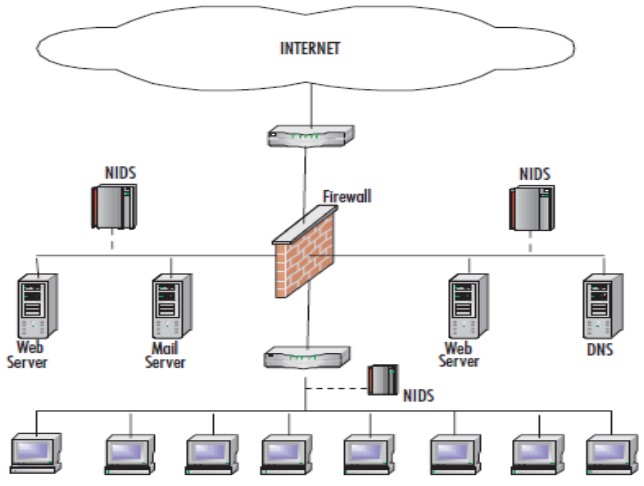


Figura 26. IDS Basados en Red (NIDS)

Elaborado por: Santiago Acosta y Jimena Muñoz

3.5.1 Ventajas de los IDS basados en Red NIDS

- Con pocos NIDS bien situados se puede controlar una red de gran tamaño.
- El despliegue de la infraestructura de NIDS tiene poco impacto en el funcionamiento de la red.
- Referente a costos, NIDS permite estrategias de instalación únicamente en los puntos críticos de la red y esto evita la utilización de tantos equipos como puntos de red exista en la red a ser implementada. Por eso el coste es menor que el uso de HIDS.
- Análisis de paquetes: los NIDS examinan todas las cabeceras de los paquetes para detectar comportamientos o actividades anómalas en el enlace de red censado.
- Interoperabilidad de sistemas operativos: se puede mencionar que los NIDS son independientes del sistema operativo que se esté ejecutando en la computadora o el dispositivo, por lo cual proporciona una gran ventaja sobre los HIDS. (Coll Almela, 2001, págs. 20,21).

3.5.2 Desventaja de los IDS basados en red NIDS.

- Pueden tener dificultades procesando todos los paquetes en una red con bastante trafico al igual que puede fallar en reconocer ataques generados durante periodos de trafico alto.
- Estos no analizan información cifrada.
- No pueden llegar a saber si el ataque tuvo éxito o no, ya que la única información que despliegan es que algún ataque fue lanzado al enlace analizado. Lo cual implica que se necesita de administradores para que manualmente puedan tratar de mitigar el ataque detectado. (Mira Alfaro, 2001, pág. 18).

3.6 Sistemas de detección de intrusos distribuidos DIDS

Éste sistema contiene varios sensores repartidos por diversos equipos y puntos de la red, los mismos que se comunicaran con un nodo central el cual recibirá toda la información relevante y donde se analizan los datos para disponer de una visión más amplia del sistema en conjunto y detectar con mayor fiabilidad los ataques. Al poseer varios sensores distribuidos por toda la red permite ampliar la información disponible para la detección

de un incidente en el sistema. En concreto, evitaría la existencia de segmentos de red aislados y no monitoreados. Esto permite producir además una única respuesta a intrusiones visibles desde varios puntos de la red. (Giménez & Gómez, 2008, pág. 18).

Sistema de detección de intrusos distribuido DIDS

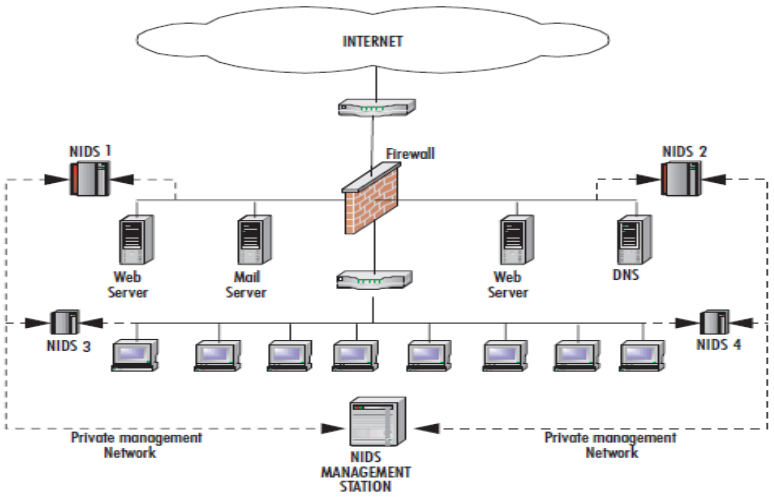


Figura 27. Sistema de detección de intrusos distribuido (DIDS)
Elaborado por: Santiago Acosta y Jimena Muñoz

3.7 Funcionamiento del IDS

Los IDS pueden utilizar una variedad de técnicas con el fin de recopilar estos datos, incluyendo la detección de paquetes generalmente en modo promiscuo para capturar datos de la red tanto como sea posible. Una vez capturado los paquetes se procede a realizar análisis los cuales tenemos los siguientes:

- **Detección de abusos o firmas:** usado para la mayoría de sistemas comerciales. Estos analizan buscando eventos que coincidan con un patrón o firma que describe un ataque conocido.
- **Detección de anomalías:** el análisis busca patrones anormales de actividad en host o en la red, estos funcionan asumiendo que los ataques son diferentes a la actividad normal. Manejan técnicas estadísticas que definen de forma aproximada lo que es el comportamiento usual o normal de la red.

Después de que el IDS ha reunido los datos, utiliza varias técnicas para encontrar las intrusiones y los intentos de intrusión. Al igual que los servidores de seguridad, un IDS puede adoptar políticas de buenos conocidos y mal conocidos.

- **Políticas de buenos conocidos:** el IDS está configurado para reconocer los datos buenos o deseados, y para alertar sobre cualquier otra cosa. Muchos de los motores de detección de anomalías abrazan este modelo, lo que provocará alertas cuando ocurre algo fuera de un conjunto definido de parámetros estadísticos.
- **Las políticas mal conocidas:** son mucho más simples, ya que no requieren de un modelo global de entrada permitida, y alertan sólo sobre datos o tráfico que se sabe que es un problema. La mayoría de los motores de IDS basados en firmas trabajan sobre modelos mal conocidos, con una base de datos cada vez mayor de firmas de ataques maliciosos.

Las políticas bien y malas conocidas pueden trabajar conjuntamente dentro de una única implementación IDS, utilizando la detección mal conocida de firmas y la detección bien conocida de anomalías de protocolo con el fin de encontrar más ataques.

Por último, se debe considerar qué hace el IDS cuando encuentra un intento de ataque. Hay dos categorías generales de respuesta:

- **Respuesta pasiva:** puede generar alertas o logs de registros pero no obstruye la manipulación de la red, es decir que no toma acciones que pueda cambiar el curso del ataque.
- **Respuesta activa**: son acciones automáticas que se toman cuando cierto tipo de intrusiones son detectados. (Beale, Baker, & Ester, 2007, pág. 9).

3.8 Snort

Es un programa IDS basado en red escrito bajo licencia GNU GPL, soporta múltiples plataformas, permite realizar análisis de los protocolos, búsquedas por patrones, en donde examinan todos y cada uno de los paquetes que reciben las distintas interfaces de red de

una máquina. Una vez adquirido, el paquete es analizado para ver si el tráfico recibido cumple alguna de las reglas establecidas por el administrador.

Snort con licencia abierta y código multiplataforma se convierte en una herramienta útil para todos los administradores de red. Esa es la razón por la que se le da el calificativo de ligero (lightweight), en comparación con los grandes NIDS comerciales. Y lo que se podría decir en cuanto a los contra de esta aplicación es que genera gran cantidad de falsos positivos, requiere bastante esfuerzo, tunning de reglas y análisis.

3.8.1 Arquitectura de Snort

Los elementos que componen el esquema básico de su arquitectura son:

- **Módulo de captura del tráfico:** es el encargado de capturar todos los paquetes de la red utilizando la librería libpcap.
- **Decodificador: s**e encarga de formar las estructuras de datos con los paquetes capturados e identificar los protocolos de enlace, de red. se encarga de tomar los paquetes de los host, los decodifica y se guardan en memoria, una vez que estos paquetes son decodificados son tratados mediante preprocesadores y luego son enviados al motor de detección.
- **Preprocesadores**: permiten extender las funcionalidades preparando los datos para la detección. Existen diferentes tipos de preprocesadores dependiendo del tráfico que se analizará.
- **Motor de detección**: analiza los paquetes en base a las reglas definidas para detectar los ataques, consiste en realizar las búsquedas de firmas, es decir, que compara los paquetes leídos con las reglas definidas, estás son agrupadas por categorías, cuando el paquete coincide con alguna de las reglas se pasa a la siguiente capa.
- **Archivo de reglas**: definen el conjunto de reglas que regirán el análisis de los paquetes detectados.
- **Plugins de detección**: partes del software que son compilados con Snort y se usan para modificar el motor de detección.

- **Plugins de salida: p**ermiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que las generaron. Pueden ser archivos de texto, bases de datos, servidor syslog, etc. (Jiménez Galindo, 2009, pág. 56).

En la Figura 28 se explica la arquitectura de Snort.

Diagrama de flujo de la arquitectura de Snort

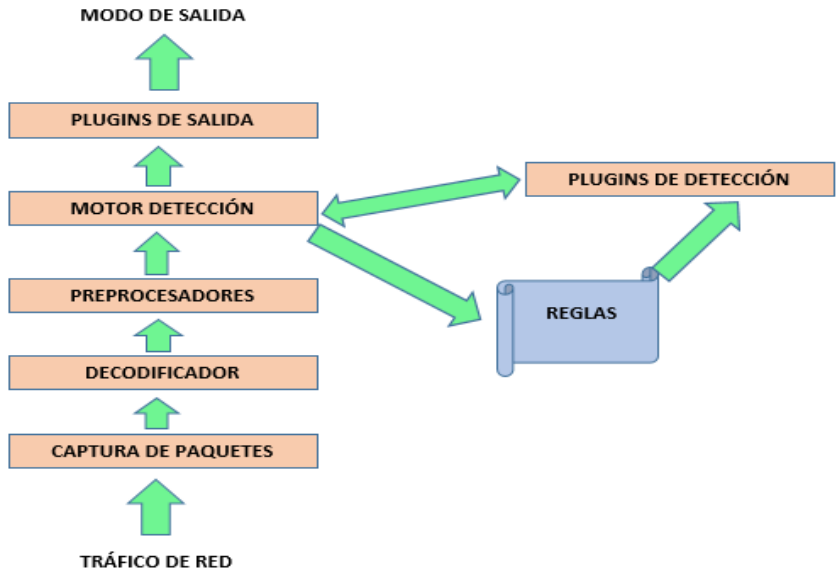


Figura 28. Arquitectura de Snort

Elaborado por: Santiago Acosta y Jimena Muñoz

3.8.2 Características de Snort

A continuación se enuncian las características que cumple Snort:

- Snort muestra o registra todos los paquetes dirigidos a su interfaz de red como a los que no le corresponda escuchar, es decir que Snort trabaja en modo promiscuo.
- Snort al escuchar en modo promiscuo en una interfaz de red y atender a una serie de reglas más avanzadas que las de tcpdump, da una gran ventaja ya que sirve para analizar y depurar tráfico y protocolos de red.
- Al utilizar una base de reglas sofisticadas para el análisis avanzado de tráfico de red, Snort detecta y alerta sobre tráfico no deseado que esté circulando por la red.

Una de sus grandes ventajas que se puede mencionar es que aparte de escuchar y sobresalir en los protocolos IP+TCP/UDP/ICMP, también es capaz de escuchar en otros protocolos tales como ethernet, fddi, arp, rarp, decnet, lat, sca, moprc y mopdl. Cuando Snort filtrar y analizar el tráfico, lleva una serie de módulos que le permiten:

- Reestructurar el tráfico fragmentado.
- Comprender el tráfico rpc.
- Detectar escaneos remotos en busca de puertos abiertos.

La gran ventaja que proporciona es que es modular y fácil de expandir su funcionalidad". (Brickmanne, p. 3).

3.8.3 Modos de Funcionamiento de Snort

Snort puede funcionar en los siguientes modos:

- **Modo sniffer**: permite mecanizar por pantalla en tiempo real toda la actividad en la red en que Snort es configurado.
- **Modo packet logger** (registro de paquetes): éste modo es el que se almacena en un sistema de log toda la actividad de la red en que se ha configurado Snort para un posterior análisis.
- **Modo IDS**: en el que se motoriza por pantalla o en un sistema basado en log, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar para estudiar los posibles ataques. (Torres V, 2012, pág. 10).

3.9 Reglas (Rules)

Las reglas también conocidas como firmas son los patrones que se buscan dentro de los paquetes de datos. Las reglas de Snort son utilizadas para comparar los paquetes recibidos y generar las alertas, las mismas que se van a disparar si existe coincidencia entre el contenido de los paquetes y las firmas. El archivo snort.conf permite llevar un gran control de las mismas permitiendo añadir o eliminar clases enteras de reglas, al final del archivo se pueden ver todos los conjuntos de reglas de alertas y si en un caso desea desactivar toda

una categoría de reglas solo hay que comentar la línea de la misma. (Sayago Giovanni, Tarazona Gustavo, 2014).

3.9.1 Categorías de reglas Snort

Para evaluar un paquete podemos destacar cuatro reglas de Snort, las mismas que se dividen en las que tienen contenido y las que no tienen contenido, a continuación de describe cada una de las reglas.

- **Reglas de protocolo**: las reglas de protocolo son reglas las cuales son dependientes del protocolo que se está analizando.
- **Reglas de contenido genéricas**: éste tipo de reglas permite especificar patrones para buscar en el campo de datos del paquete, dichos patrones de búsqueda pueden ser binarios o en modo ASCII.
- **Reglas de paquetes malformados:** éstas reglas se centran en especificar características sobre los paquetes, concretamente sobre sus cabeceras las cuales indican que se está produciendo algún tipo de anomalía, este tipo de reglas no miran el contenido ya que primero se comprueban las cabeceras en busca de incoherencias u otro tipo de anomalía.
- **Reglas IP**: éste tipo de reglas se basa directamente sobre la capa IP y son comprobadas para cada datagrama IP, si el datagrama luego es Tcp, Udp o Icmp se realizará un análisis del datagrama con su correspondiente capa de protocolo, este tipo de reglas analiza con contenido y sin él. (Jiménez Galindo, 2009).

3.9.2 Estructura de las reglas de Snort

Las reglas de Snort están formadas básicamente de dos partes fundamentales que son:

- La cabecera
- Las opciones

En la Figura 29 se puede ver de manera gráfica las partes que componen una regla Snort.

Diagrama de las partes que conforman una regla de Snort

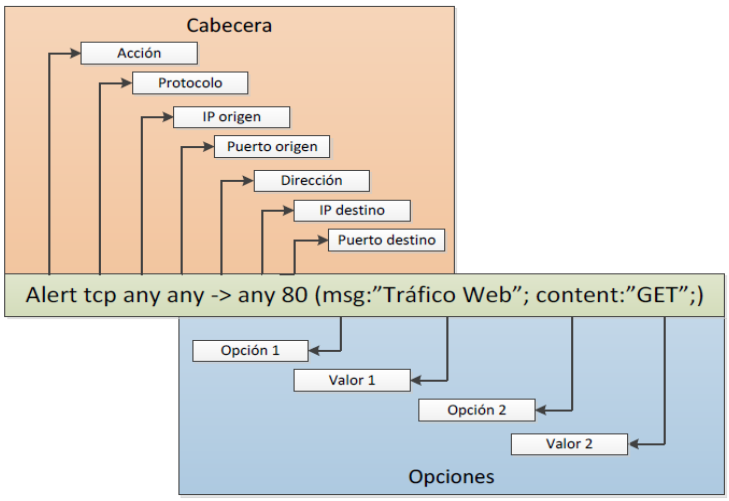


Figura 29. Partes de la regla de Snort

Elaborado por: Santiago Acosta y Jimena Muñoz

La función principal de la cabecera es identificar el tráfico de la dirección IP y el puerto con la acción que va a realizar el mismo, es decir, que puede sensar diferentes tipos de tráfico según sea especificado en la regla, en la parte de las opciones contiene condiciones específicas para analizar de forma más detallada el tráfico. (Arteaga Delgado & Atiaga Galeas, 2013, pág. 85).

3.9.3 Cabecera de la regla de Snort

Como se puede apreciar en la Figura 29, las partes que componen la cabecera son: acción, protocolo, dirección IP origen, puerto origen, dirección, dirección IP destino, puerto destino.

- **Acción*:*** indica lo que se va hacer en el paquete, el cual puede tener las siguientes acciones:
  - ***pass**:* Sort debe ignorar el paquete
  - ***log**:* Snort debe generara un log del paquete que se enlace con una regla.
  - ***alert**:* se generara una alerta y un log del evento detectado.

- ***activate**:* usado para generar una alerta y activar otra regla para verificar si la naturaleza del tráfico es legítima.
- ***dynamic**:* este tipo es únicamente activada por regla con acción "Activate", brinda la facilidad de realizar reglas con mayor complejidad con el objetivo de disminuir la cantidad de falsos positivos.
- ***acciones definidas por el usuario**:* Snort permite a los usuarios crear acciones personalizadas.

- **Protocolo*:*** busca paquetes según el protocolo que haya sido configurado los cuales pueden ser:
  - TCP, UDP, ICMP, IP, Any

- **Dirección IP y puertos origen y destino*:*** en estos parámetros se deben especificar los valores que se desee para que la alerta se ejecute, se configura "any" para todo lo definido por el usuario.

- **Dirección*:*** indica el flujo del tráfico desde el origen hacia el destino y se lo puede configurar de dos maneras:
  - ***Unidireccional**:* la dirección ip y el puerto de la izquierda son origen y la dirección ip y puerto de la derecha es destino, la simbolización usada es "->".
  - ***Bidireccional**:* genera que el evento se dispare en cualquier flujo de datos que contenga las direcciones IP y puertos especificados, la simbología es "<>". (Arteaga Delgado & Atiaga Galeas, 2013, pág. 86)

3.9.4 Opciones de la regla de Snort

La sección de opciones es donde la regla se vuelve eficiente, cada acción que se vaya a realizar va seguida del símbolo ":" más la opción que se va a configurar en la opción.

Las palabras claves que se tiene para configurar son:

- ***msg**:* mensaje que se mostrará al momento que se genere una alerta.

- ***sid:*** número identificador de las reglas de Snort, entre 0 y 99 son reservadas para usos futuros, entre 100 y 1000000 son reglas de distribución oficial de Snort, a partir de la 1000001 se puede usar para reglas personalizadas.
- ***logto****:* debe crear un log en un archivo o base de datos específica.
- ***minfrag****:* configura un indicio del mínimo tamaño de fragmentación de un paquete.
- ***dsize****:* configura tamaño de la carga útil del paquete, se puede usar símbolos de mayor o menor que.
- ***content****:* busca un patrón determinado dentro de la carga útil del paquete.
- ***flags****:* busca por banderas TCP configuradas en determinados valores.
- ***seq****:* buscar número de secuencia TCP específico.
- ***ack****:* busca campo acknowledge dentro de la cabecera TCP.
- ***itype****:* busca campo ICMP type dentro de la cabecera del paquete.
- ***offset****:* es el modificador de la opción "content", configurado para la búsqueda de un patrón específico.
- ***ttl****:* busca patrón Time-to-Live en la cabecera del paquete.
- ***id****:* busca determinadas opciones ip dentro de la cabecera ip, las más usadas son: Record Route (rr), Time Stamps (ts), Loose Source Routing (lssr), Strict Source Routing (ssrr).
- ***pcre****:* permite usar expresiones regulares en perl para búsqueda de patrones dentro de la cara útil del paquete.

Para tener un ejemplo claro de la aplicación de la estructura de la regla en un ejemplo real creado para futuros análisis con una regla personalizada, se puede apreciar en la Figura 30, en la cual como acción se tiene alert para generar una alerta, con el protocolo tcp, en lo que se refiere dirección y puerto de origen y destino se pone con "any" para que procese tráfico de todo tipo, en el msg se mostrara el mensaje a desplegar en el momento que se detecte la amenaza y como sid se ha tomado un rango para tener como monitoreo futuro.

Creacion de una regla de Snort personalizada

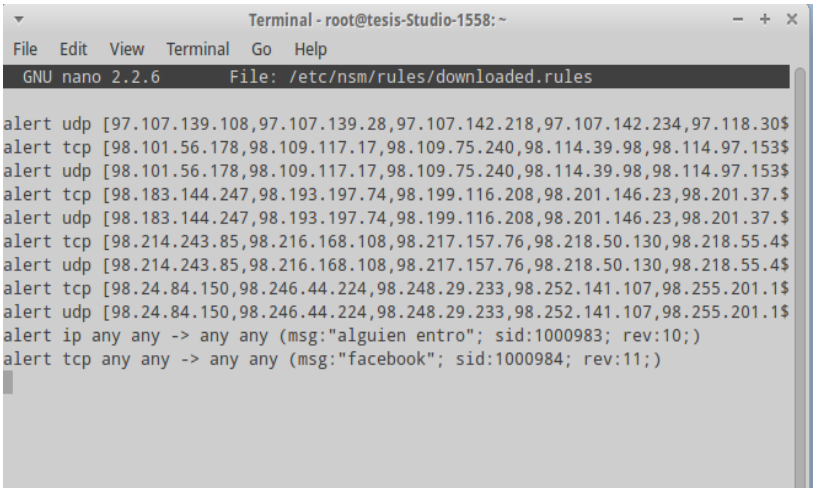


Figura 30. Alerta personalizada
Elaborado por: Santiago Acosta y Jimena Muñoz

3.10 Security Onion

Security Onion es una distribución de Linux basada en Xubuntu con el objetivo de lograr un control de seguridad de la red, básicamente se refiere a la detección de intrusos y gestión de registros para monitorización del tráfico de la red. Contiene las siguientes herramientas: Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA y muchas otras herramientas de seguridad.

Su funcionamiento se basa en la captura de los paquetes que atraviesan los sensores, en este caso el trabajo de capturar lo realizará las sondas Raspberry Pi o Sondas Pi y posterior del análisis de los paquetes se presentará las alertas recolectadas en una interfaz gráfica llamada Snorby.

3.10.1 Ventajas y desventajas de Security Onion

Las ventajas de Security Onion son:

- La Interfaz de usuario es simple y de igual manera sencilla de usar.
- La instalación no es complicada es más automatizada.

Las desventajas de Security Onion son:

- Se tiene que instalar forzadamente toda la distribución, no es posible instalar las herramientas de Security Onion por si solas.
- No es posible elegir que aplicaciones se desea instalar.
- Alta demanda de recurso.

3.10.2 Escenarios de instalación de Security Onion

Security Onion tiene tres modos principales de instalación los cuales son:

- Instalación Independiente
- Instalación Servidor-Sensor
- Instalación Híbrido (Security Onion, 2013)

3.10.2.1 Instalación independiente (Standalone)

Este tipo de instalación consta de una maquina ya sea física o virtual en la cual pueden correr componentes tanto del servidor como del sensor y procesos relacionados. La instalación independiente puede tener múltiples interfaces que monitorean varios segmentos de red. Esta instalación es la más sencilla y conveniente para monitorear la red que son accesibles por esta única localización.

3.10.2.2 Instalación Servidor-Sensor

Constituye de una sola maquina la cual procede a ejecutar los componentes de servidor con una o más maquinas separadas ejecutándose como sensor y reporta al servidor los eventos capturados. Éste modo de instalación reduce el tráfico de red, manteniendo la mayor parte de los datos guardados en los sensores hasta que lo requiera el servidor para analizar.

3.10.2.3 Instalación híbrido

Una instalación híbrida consiste en una instalación independiente que solo tiene uno o más sensores separados que reportan al servidor de la maquina independiente.

3.10.3 Instalación del escenario de Security Onion

En esta parte se especifica primero los requerimientos mínimos de hardware que debería tener el servidor que está cargado con Secuity Onion, sus requerimientos son:

- Disponible para 32 bits y 64 bits
- RAM mínimo de 4 GB
- HD mínimo de 520 GB

Nota: para el almacenamiento de la captura de paquetes completos que lo realiza Security Onion, es necesario una gran capacidad de almacenamiento.

La instalación del escenario que se va a usar en el desarrollo de este proyecto de titulación se lo explicará en los siguientes pasos:

- Para la instalación del IDS en Security Onion primero se da doble click sobre el setup de instalación que se encuentra en el escritorio, como se muestra en la Figura 31, se aprecia la interacción entre sistema y proceso de instalación.
- Elegir yes para configurar las interfaces de red.

Configuración de Security Onion con respecto a la tarjeta de red

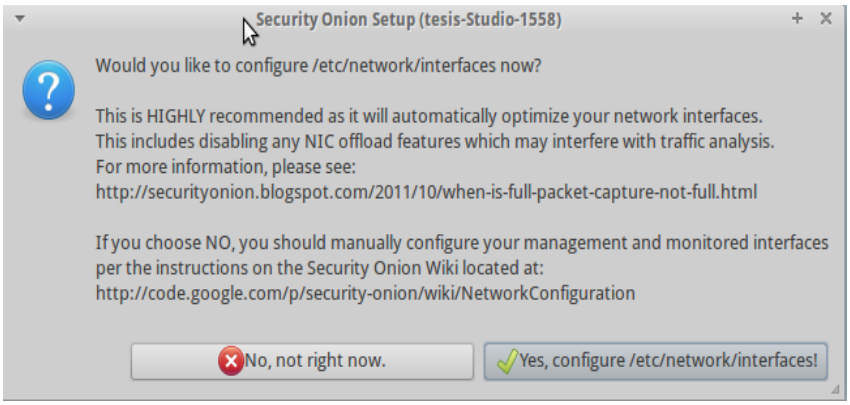


Figura 31. *Configuración de la interfaz de red*
Elaborado por: Santiago Acosta y Jimena Muñoz

- Elegir la configuración de la interfaz si se desea DHCP o estática. En la Figura 32 se puede ver el cuadro para elección de la configuración.

Configuración de la tarjeta de red en modo DHCP

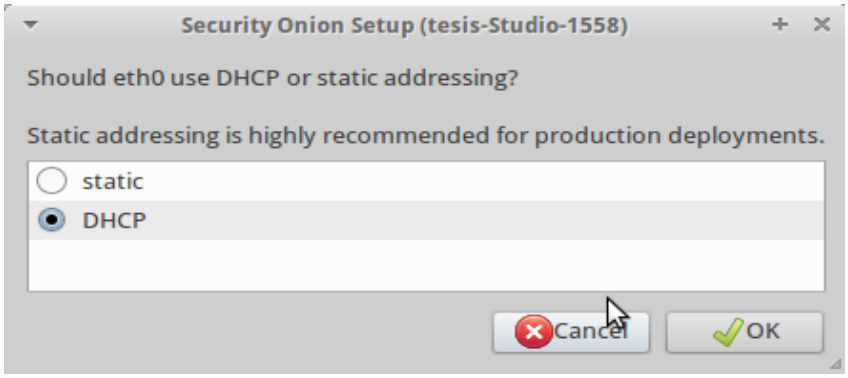


Figura 32. Configuración de tarjeta de red

Elaborado por: Santiago Acosta y Jimena Muñoz

- Reiniciar el sistema operativo. Se da doble clic en el setup de y seleccionar la opción ***Advanced Setup.*** Después continuar con las configuraciones por defecto según el requerimiento. Se puede apreciar las opciones en la Figura 33.

Configuración avanzada de la instalación de Security Onion

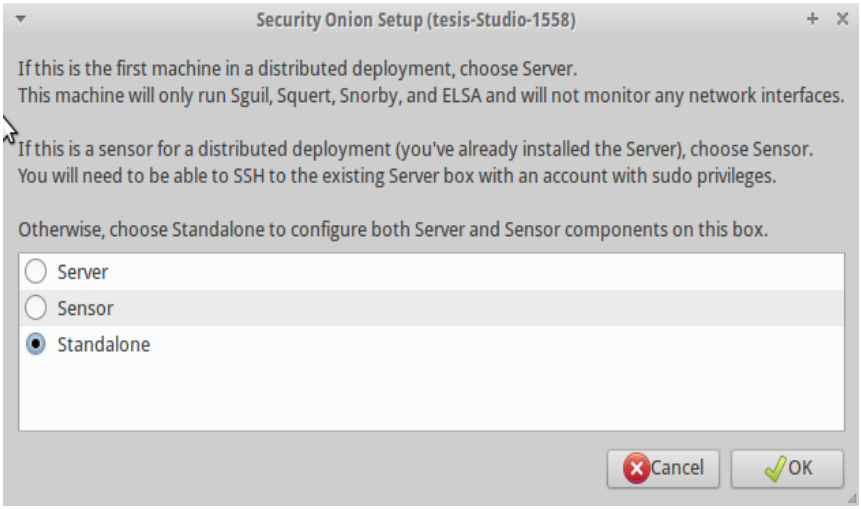


Figura 33. Configuración avanzada

Elaborado por: Santiago Acosta y Jimena Muñoz

- Elegir el motor de IDS que se va a elegir en este caso es Snort. Seguir con las configuraciones por defecto y reiniciar el sistema. En la Figura 34 se puede ver las opciones del motor de IDS a ser configurado.

Instalación del motor de IDS de Snort

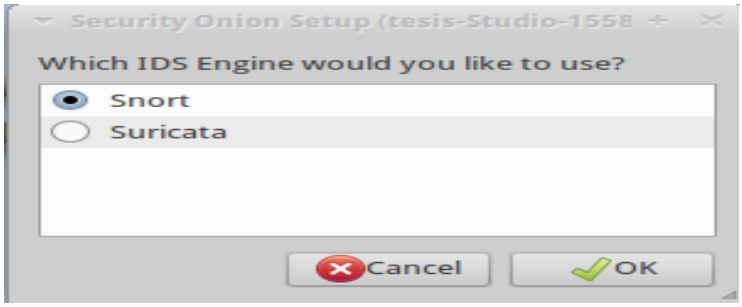


Figura 34. Instalación de motor de IDS

Elaborado por: Santiago Acosta y Jimena Muñoz

- Una vez ya instalado el motor de IDS, se verifica que se genera las carpetas de Snort con el conjunto de reglas que contiene Snort ubicadas en la carpeta /etc/nsm/rules. En la Figura 35 se puede observar la carpeta antes mencionada con los archivos de las reglas.

Ubicación de la carpeta que contiene las reglas de Snort

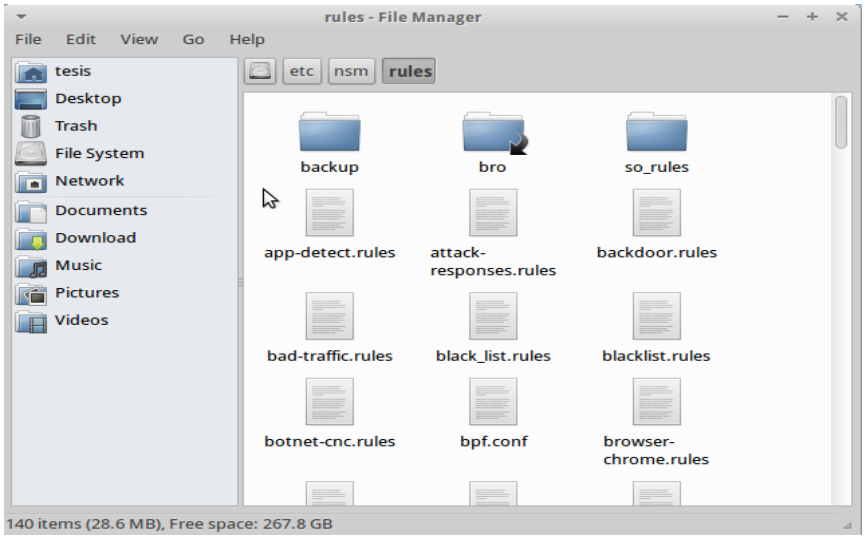


Figura 35. Ubicación de reglas de Snort
Elaborado por: Santiago Acosta y Jimena Muñoz

- En la configuración de la tarjeta de red se procede a configurar con ip's estáticas, en la cual va a tener dos enlaces de red; uno de ellos va a ser para la interfaz de administración y el otro es para el monitoreo; de igual manera se podrá apreciar la interfaz de las Sondas Pi. En la Figura 36 se especifica la configuración de la interfaz.

Configuración de las ip para la tarjeta de red del servidor

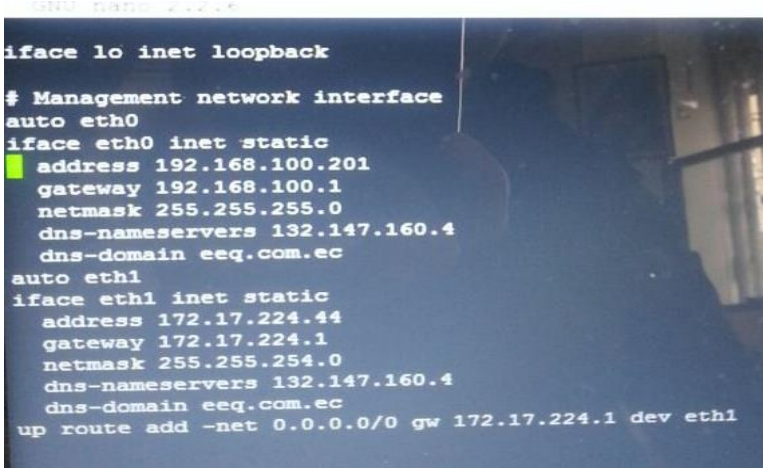


Figura 36. Configuración de la tarjeta de red del servidor

Elaborado por: Santiago Acosta y Jimena Muñoz

3.11 Kali Linux

Kali Linux es usado para realizar todo tipo de auditoria de seguridad y pruebas de penetración de intrusos. Kali Linux es una plataforma basada en GNU/Linux Debian la cual es la versión actual reconstruida de BackTrack, cuenta con herramientas muy importantes para capturar información, identificar vulnerabilidades, escalar privilegios y cubrir huellas. (Caballero, 2015, pág. 9).

3.11.1 Características de Kali Linux

Al ser una reconstrucción completa de BackTrack y basada en plataforma de Debian con las herramientas nativas de la versión anterior tiene las siguientes características:

- Más de 300 herramientas de pruebas de penetración de intrusos.
- Es una distribución libre.

- Tiene amplio soporte para dispositivos inalámbricos.
- Parches de Kernel para inyección.
- Es multi-lenguaje.

Con todo lo enunciado en los puntos anteriores esta distribución fue elegida para este proyecto de titulación porque es muy estable para el uso de seguridad de redes o específicamente en el tema de Sistemas de Detección de Intrusos (IDS). (Caballero, 2015, pág. 9).

3.12 Configuración de las Sondas PI

En este punto se procederá con los comandos y configuraciones de las Sondas Pi también llamadas Raspberry Pi. Después de haber instalado el sistema operativo Kali Linux el cual fue elegido como sistema operativo de las sondas se hace lo siguiente:

- Primero se procede con la actualización del sistema operativo y a instalar las operaciones de control con *openssh*. En la Tabla 14 se especifica los comandos para la actualización del sistema operativo.

Tabla 14. *Instalación de paquetes de actualización*

Comando	Descripción
sudo apt-get update	Actualiza lista de paquetes y sus versiones; pero no instala ni actualiza ningún paquete.
sudo apt-get upgrade –y	Después de ejecutar el comando anterior este comando instala y actualiza dichos paquetes.
sudo apt-get install -y openssh–server	Se instalará OpenSSH que proporciona un demonio servidor y herramientas de cliente para facilitar las operaciones de control y transferencia de archivos remotamente, seguras y codificadas. La opción –y se refiere a: no pregunta y asume que si a todo.
sudo reboot	Reiniciará el sistema.

Nota. Cuadro contiene paquetes necesarios para iniciar con instalación de Snort.
Elaborado por: Santiago Acosta y Jimena Muñoz

3.12.1 Configuración de la tarjeta de red

- En la configuración de la tarjeta de red se debe configurar con IP estáticas, de acuerdo al análisis anteriormente realizado se eligió el enlace del Wireless Controler que está asociado a la vlan13, en la figura 38 se especifica las IP asignadas a la Sonda pi de monitoreo.

Configuración de la tarjeta de red de la Sonda Pi

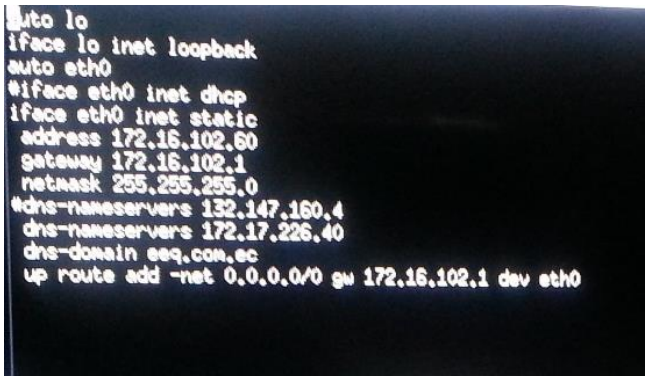


Figura 37. Configuración de la tarjeta de red de Sonda Pi

Elaborado por: Santiago Acosta y Jimena Muñoz

3.12.2 Instalación de los pre-requisitos de Snort

Para la instalación de Snort se requiere algunos requisitos importantes que están habilitados para la Debian.

Tabla 15. *Instalación de pre-requisitos de Snort*

Comando	Descripción
sudo apt-get install -y build-essential	Este comando instala las herramientas necesarias para construir software.
sudo apt - get install -y libpcap - dev libpcre3 - dev libdumbnet –dev	Se procede a instalar los pre-requisitos que solicita Snort.

	libpcap: es una librería para captura de paquetes a nivel de usuario. ***libpcre3***: es una biblioteca de funciones que admite las expresiones habituales de Perl 5. ***Libdumbnet:*** proporciona una interfaz simplificada, portátil para varias rutinas de redes de bajo nivel.

Nota. Instalación de los pre-requisitos que necesita Snort.
Elaborado por: Santiago Acosta y Jimena Muñoz

- Crear una carpeta en la cual se descargara y guardara los paquetes en esta carpeta e ingresar a dicha carpeta.
    - mkdir ~/ snort_src
    - cd ~/ snort_src

3.12.3 Instalación de DAQ (librería de adquisición de satos)

DAQ es esencialmente una capa de abstracción y una suite de módulos interconectados que se pueden seleccionar en tiempo de ejecución. Haciendo que el cambio de modo pasivo en línea sea fácil, y no requiera recopilación del núcleo de Snort.

- Se instala los siguientes requisitos que se especifican en la Tabla 16:

Tabla 16. *Instalación de DAQ*

Comando	Descripción
sudo apt-get install -y bison flex	Instalar bison y flex ***flex:*** herramienta que genera analizadores léxicos a partir de un conjunto de expresiones regulares. ***bison***: herramienta que genera analizadores sintácticos.

wget https://www.snort.org/downloads/snort/daq-2.0.4.tar.gz	Comando para descargar DAQ. ***wget***: permite descargas desde la Web.
tar -xvzf daq-2.0.4.tar.gz	Descomprime el paquete .tar de DAQ.
cd daq-2.0.4	Ingresar a la carpeta de daq descomprimida
./configure	***./configure***: configura y crea un fichero 'Makefile' que será utilizado por 'make' para compilar/instalar el programa.
Make	make permite realizar la compilación.
sudo make install	Se procederá a instalar la compilación.

Nota. Descripción de cómo se debe instalar DAQ.

Elaborado por: Santiago Acosta y Jimena Muñoz

3.13 Montaje del NFS servidor y Sonda PI

"NFS o Network File System, protocolo de sistema de archivos distribuido que permite montar directorios remotos en el servidor. Esto permite aprovechar el espacio de almacenamiento en un lugar diferente y escribir en el mismo espacio desde múltiples servidores". (Ellingwood, 2014).

Para la configuración del DIDS se va a levantar el NFS entre servidor y cliente para leer el set de reglas de Snort desde las Sondas Pi hacia el servidor y posteriormente escribir los eventos en la base de datos del servidor.

3.13.1 Descargar e instalación de los componentes de NFS

- En el servidor se descargará los paquetes necesarios para la instalación del NFS, con el siguiente comando se procede con la instalación:
    - *sudo apt-get install nfs-kernel-server*

- En lo referente a la Sonda Pi se instala el componente del NFS como cliente con el siguiente comando:
    - *sudo apt-get install nfs-common*

- Configure las exportaciones NFS, abrir el directorio /etc/exports con el editor de texto con privilegios de root en el servidor:

    - *sudo nano /etc/exports*

- En el fichero /etc/exports se crea una línea para cada uno de los directorios que se desea compartir, En la Figura 38, se muestra al archivo /etc/exports editado y en la parte final del mismo como quedara la línea del directorio compartido en este caso es:

    /etc/nsm/rules: representa la ruta o directorio a ser compartido.

- 192.168.1.6: corresponde a la IP del equipo donde va ser compartido.

Configuracion del directorio que se monta el NFS

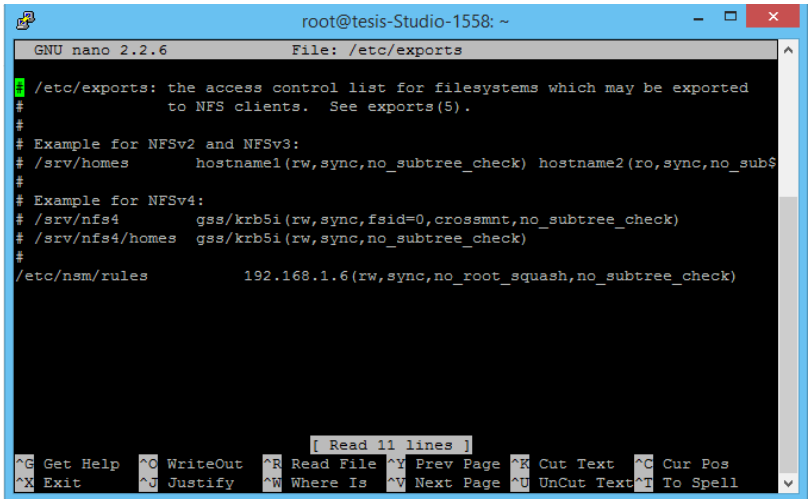


Figura 38. Configuración de directorio /etc/exports
Elaborado por: Santiago Acosta y Jimena Muñoz

- El servicio NFS se debe levantar del ser4vicio de NFS con el siguiente comando:
    - *sudo service nfs-kernel-server start*
- A continuación se procederá a montar en la Sonda Pi el NFS, con el siguiente comando.
    - *sudo mount dirección_ip_servidor:/directorio_a_compartir_o_montar" /directorio_donde_va_estar_el_directorio_del_servidor*

    Ejemplo: sudo mount 172.17.224.5:/etc/nsm/rules /root/Desktop/rules_server

3.14 Instalación de Snort

- Para la instalación de Snort se requiere de los siguientes comandos que se especifican en la Tabla 17:

Tabla 17. *Instalación de Snort*

Comando	Descripción
cd ~/ snort_src	Se debe ingresar a la carpeta de descargas.
wget https://www.snort.org/downloads/snort/ snort-2.9.7.0.tar.gz	Se procede a descargar el archivo snort-2.9.7.0 con el comando wget.
tar -xvzf snort-2.9.7.0.tar.gz	Descomprimir paquete de Snort.
cd snort -2.9.7.0	Ingresar a la carpeta de Snort
./ configure --enable-sourcefire	La opción --enable-sourcefire, da el monitoreo de desempeño de paquetes, que permite el monitoreo del desempeño de las reglas y preprocesadores.
make	make permite realizar la compilación.
sudo make install	Se realizar la compilación y de igual manera se procederá a ser instalado.

Nota. Descripción de cómo se debe instalar Snort.

Elaborado por: Santiago Aosta y Jimena Muñoz

- Actualizar las librerías compartidas
    - *sudo ldconfig*

ldconfig: es un programa que se utiliza para mantener la caché de biblioteca compartida.

- Con el siguiente comando se verifica la versión que está instalada de Snort.
    - *snort –V*

Al momento que se ejecuta e comando snort –V, se puede observar en la Figura 39 la versión que se instaló de Snort, donde se presenta una breve resumen del mismo en este caso se observa la versión, la utilización del libcap, entre otras descripciones.

Versión que se encuentra instalada de Snort

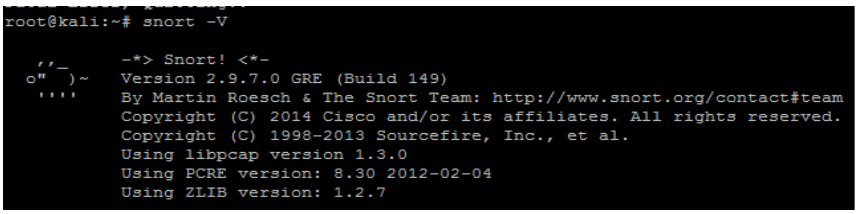


Figura 39. Desplegar versión de Snort
Elaborado por: Santiago Acosta y Jimena Muñoz

3.15 Configuración de Snort para ejecutar en modo NIDS

Dado que no se desea que Snort se ejecute como root, hay que configurar una cuenta y grupo sin privilegios para el demonio (daemon) para ejecutarse bajo (snort:snort). Se creara una serie de archivos y directorios requeridos por Snort, y establecer permisos en esos archivos. Snort mantendrá todas las configuraciones de archivos en /etc/snort, y todas las alertas se escribirá en /var/log/snort.

sudo groupadd snort

- Se crea un nuevo grupo en el sistema, en este caso se llamado snort.
    - *sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort*

El comando useradd: añade usuarios donde el -r indica que la cuenta se convierte en cuenta del sistema, -s permite modificar la shell de inicio de sesión del usuario, por defecto/bin/bash, -c indica añadir un comentario al usuario, como puede ser su nombre real y finalmente el –g el cual nos indicara el grupo al que va a pertenecer el usuario, en este caso el grupo debe de estar previamente creado.

- Se crea con comando ***mkdir*** los directorios para las reglas de Snort
    - *sudo mkdir /etc/Snort*
    - *sudo mkdir /etc/snort/rules*
    - *sudo mkdir /etc/snort/preproc_rules*
    - *sudo mkdir /var/log/Snort*
    - *sudo mkdir /usr/local/lib/snort_dynamicrules*

- ***El comando chmod:*** permitirá cambiar los permisos de un fichero o directorio, con la opción -R aplica a todos los ficheros y de los subdirectorios. Donde el número 5 nos indica que permitirá tener escritura y ejecución y el número 7 a todos los permisos en este caso lectura, escritura y ejecución.
    - *sudo chmod -R 5775 /etc/snort*
    - *sudo chmod -R 5775 /var/log/snort*
    - *sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules*

- ***El comando chown***: permite cambiar el propietario de un archivo(s) o carpetas(s), con la opción –R**, i**ndicara que los cambios se le deben de aplicar tanto a la carpeta especificada como a los archivos y subcarpetas.
    - *sudo chown -R snort:snort /etc/snort*
    - *sudo chown -R snort:snort /var/log/snort*
    - *sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules*

- Snort necesita copiar los archivos de configuración de la fuente de Snort extraído de la carpeta de: /etc/snort

    - *sudo cp ~/snort_src/snort-2.9.7.0/etc /*.conf * /etc/Snort*
    - *sudo cp ~/snort_src/snort-2.9.7.0/etc /*.map /etc/snort*

    Con el comando cp: se copiara los ficheros .conf y .map hacia los ficheros de destino que son /etc/snort y /etc/Snort

- Se Ingresa al archivo snort.conf con el comando nano para realizar los siguientes cambios, en la Tabla 18 se presenta la configuración necesaria para que se ejecute Snort según el enlace de red que se desee sensar.

    Tabla 18. *Configuración del archivo snort.conf*

Comando	Descripción
sudo nano /etc/snort/snort.conf	Se usa nano para editar el archivo de configuración snort.conf
ipvar HOME_NET 172.16.0.0/24	En este archivo se configura la línea de HOME_NET con la ip de red interna a ser sensada.

ipvar EXTERNAL_NET !$HOME_NET	Se configura la red externa para que sense todo excepto la red interna.
var RULE_PATH /root/Desktop/rules_server var SO_RULE_PATH /root/Desktop/rules_server var PREPROC_RULE_PATH /root/Desktop/rules_server var WHITE_LIST_PATH /root/Desktop/rules_server var BLACK_LIST_PATH /root/Desktop/rules_server	Se cambia las rutas para que las reglas del Snort sean leídas al ser ejecutadas con la carpeta que se levantó con NFS.
output unified2:filename snort.u2, limit 128	Con esta configuración se le indica a Snort que escriba las alertas en un fichero snort.log un tamaño máximo de 128MB cada uno. El ***.u2*** se trata de un formato uified2 que un formato binario optimizado que le permitirá a Snort generar las alertas de una forma más rápida y en un fichero más liviano para escribir en la base de datos.

Nota. Cuadro de modificaciones del archivo snort.conf

Elaborado por: Santiago Acosta y Jimena Muñoz

Se puede observar que en la Figura 40, muestra cómo quedarán las variables var con las rutas de las reglas que el Snort que serán leídas en la sonda Pi.

Archivo de configuración de Snort

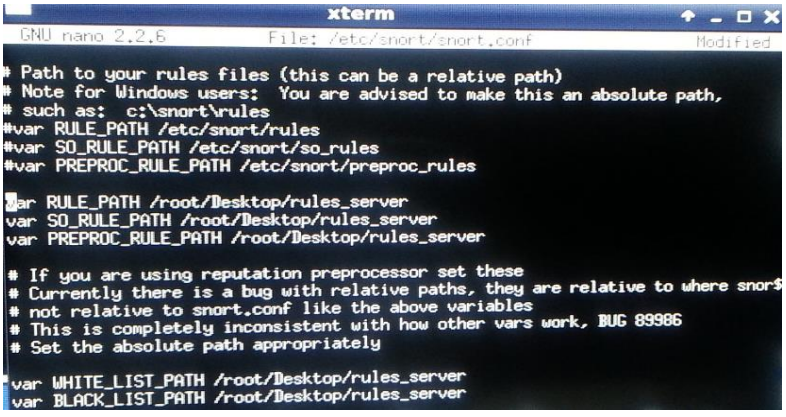


Figura 40. Configuración del archivo snort.conf

Elaborado por: Santiago Acosta y Jimena Muñoz

- Para verificar si Snort está funcionando correctamente, se usará la bandera -T para probar el archivo de configuración snort.conf esta correcto y usamos la opción -c para indicar la ruta de ubicación del archivo de configuración de Snort, si todo está correctos daría successfully con el siguiente comando:
    - *sudo snort -T -c /etc/snort/snort.conf*

Verificación de funcionamiento de Snort

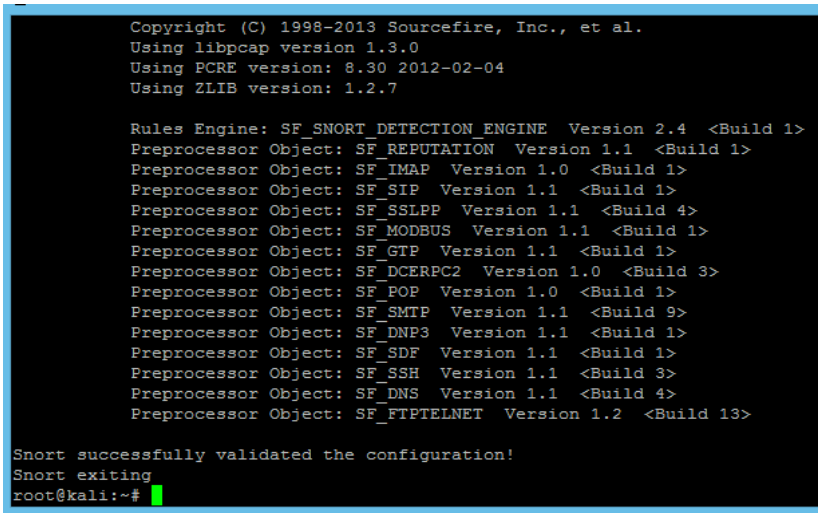


Figura 41. Funcionamiento correcto del Snort
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 41, se observa el correcto funcionamiento del Snort, como se puede observar en el mensaje de salida "Snort successfully validated the configuration" indicando que dicho archivo funciona correctamente.

- En esta etapa, Snort no tiene ninguna regla cargada localmente por ende se procede a ingresar a la carpeta compartida con NFS para censar los enlaces de red la cual toma el set de reglas de Snort que se encuentra en el servidor, para verificar que esta compartida la carpeta de reglas de ejecuta el comando:
    - df –h

Para asegurarse que los archivos o directorios se encuentran compartido en la Sonda Pi, en la Figura 42, se presenta un resumen donde se puede observar en la parte inferior de la figura, la dirección IP del equipo que está permitiendo compartir o

mantada seguido de la dirección del archivo o directorio. Esta es la dirección que se va a tomar para configurar en la sonda para poder acceder al ser de reglas de Snort del servidor.

Verificación de la dirección de montaje del NFS

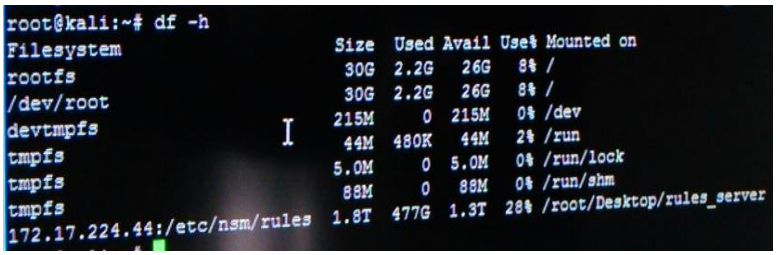


Figura 42. Comprobación del montaje en la sonda PI.

Elaborado por: Santiago Acosta y Jimena Muñoz

3.16 Barndyard2

Barnyard2 mejora la eficiencia de Snort mediante la reducción de la carga en el motor de detección principal. Lee archivos de salida de registro unificado de Snort y entra en la base de datos de ellos. (Linux Digest, 2014).

3.16.1 Instalación de los pre-requisitos de barndyard2

En esta parte se requiere primeramente instalar algunos pre-requisitos para el funcionamiento correcto de Barnyard2, se procederá a instalar el servidor de Mysql con el siguiente comando:

sudo apt-get install -y mysql-server

En esta parte se presentara de manera gráfica la configuración de mysql solicitado contraseña, en este caso se usará como password: root. En la Figura 43 se aprecia la interfaz de configuración del servidor de Mysql, el cual pide que se asigne una contraseña.

Configiracion de la contraseña de Mysql

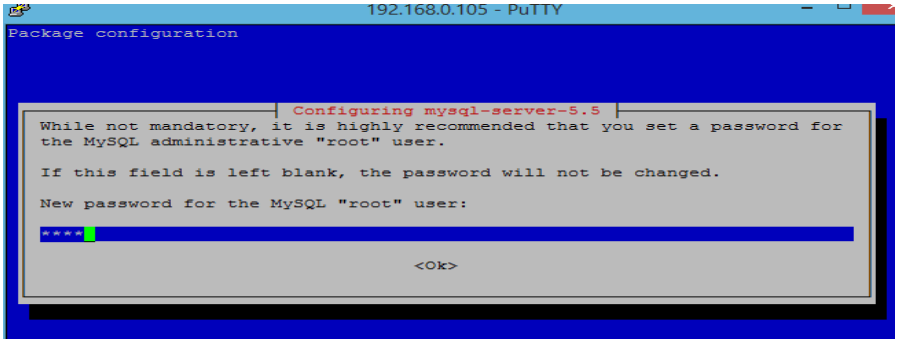


Figura 43. Ingreso de contraseña de usuario de root para MYSQL
Elaborado por: Santiago Acosta y Jimena Muñoz

En la Tabla 19 se detalla los comandos que se usarán para la instalación de los pre-requisitos de Barnyard2.

Tabla 19. *Instalación de pre-requisitos de Barnyard2*

Comando	Descripción
sudo apt-get install -y libmysqlclient-dev	***libmysqlclient-dev***: paquete que incluye las bibliotecas de desarrollo y archivos de cabecera.
sudo apt-get install -y mysql–client	Mysql-client: incluye los binarios del cliente y las herramientas adicionales innotop y mysqlreport.
sudo apt-get install -y m autoconf	***autoconf:*** es un paquete con licencia el cual produce un shell script "configure" para generar una cabecera Makefile.
sudo apt-get install -y libtool	***libtool:*** permite añadir los nuevos comandos de construcción en la biblioteca genérica a su Makefile.

Nota. Estos pre-requisitos son para que barnyard2 corra sin problemas.

Elaborado por: Santiago Acosta y Jimena Muñoz

3.16.2 Descargar e instalación de Barnyard2

Para la descarga de Barnyard2 y posteriores instalaciones se va hacer en la carpeta ~/snort_src, a continuación se indica los comandos necesarios para dicha descarga e estación, y en la Tabla 20se detalla los comandos de instalación de Barnyard2.

Tabla 20. *Instalación de Barnyard2*

Comando	Descripción
wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-2-1.13.tar.gz	Con el comando wget se procede a descargar el archivo barnyard2-2-1.13.tar.gz
tar zxvf barnyard2 -2-1.13.tar.gz	Este comando descomprime el paquete de barnyard2
cd barnyard2-master	Se ingresa al directorio barnyard2-master.
autoreconf -fvi -I ./m4	***El autoreconf***: ejecuta automáticamente, y en el orden correcto, autoconf, autoheader, aclocal, automake, y libtoolize para ahorrar tiempo cuando se hacen cambios en las plantillas de autoconf y automake.
./configure --with-mysql --with-mysql-libraries=/usr/lib/arm-linux-gnueabi	***./configure***: es el encargado de configurar y crear un fichero 'Makefile' que será utilizado por 'make' para compilar/instalar el programa que estas instalando.
sudo apt-get install -y libdnet sudo apt-get install -y libdnet-dev sudo apt-get install -y libdumbnet sudo apt-get install -y libdumbnet-dev sudo apt-get install -y libpcap sudo apt-get install -y libpcap-dev sudo apt-get install -y libgtk2.0-0 sudo apt-get install -y libgtk2.0-dev sudo apt-get install -y libgtk2.0-bin sudo apt-get install -y libgtk2.0-common sudo apt-get install -y libglib2.0-data sudo apt-get install -y libglib2.0-dev sudo apt-get install -y libglade2-0 sudo apt-get install -y libglade2-dev	Se instala las siguientes librerías que barnyard2 necesita
chmod 755 configure	Este comando se dará permisos al archivo de configuración para compilarlo e instalar barnyard2.
./configure	Se configura y se crea el fichero “Makefile” con el comando ./configure, para ser será utilizado por el 'make' el cual compilar/instalar el programa que está instalando.

Make sudo make install	***El comando make***: permitirá realizar la compilación para posterior realizar la instalación del mismo.
sudo cp etc/barnyard2.conf /etc/snort	Ingresar al directorio barnyard2-master con el comando cd, y copiar el archivo de configuracion de barnyard2 en el directorio de snort
sudo mkdir /var/log/barnyard2	Se crea el directorio que contendrá los log de barnyard2
sudo chown snort.snort/var/log/barnyard2 sudo touch /var/log/snort/barnyard2.waldo sudo chown snort.snort/var/log/snort/barnyard2.waldo sudo touch /etc/snort/sid-msg.map	El comando chown, permite cambiar el propietario de un archivo(s) o carpetas(s), y con el comando touch permite crear archivos vacíos.
sudo nano /etc/snort/barnyard2.conf	Ingresar a la configuración de barnyard2, en este archivo se deba apuntar a la base de datos que se encuentra en el servidor y a la ip del servidor. ***database: log, mysql, user=snort password=passnort dbname=snorby host=172.17.224.44***

Nota. Cuadro explicativo de la instalación de Barnyard2

Elaborado por: Santiago Acosta y Jimena Muñoz

3.16.3 Pruebas de Funcionamiento de Barnyard2

Para verifica que barnyard2 está funcionando correctamente se tiene que escribir los eventos en un archivo binario log, y que el barnyard2 lea estos logs y escriba los eventos en nuestra base de datos. Se iniciara ambos programas en modo daemon "demonio" y generar algunos eventos haciendo ping a la interfaz. Correr en modo de alerta a Snort. Las opciones que muestra este comando –u snort ejecuta el grupo, -u snort se ejecuta como usuario Snort, -c hace referencia a la dirección del archivo de configuración de snort.conf y –i monitorea la interfaz que está escuchando. El archivo binario que crea barnyard2 es de extensión .u2

sudo /usr/local/bin/Snort –q –u snort –g snort –c /etc/snort/snort.conf –i eth0

- Para escribir los eventos generados por el archivo .u2 que se obtuvo del comando anterior se ejecuta el siguiente comando para escribir esos eventos en la base de datos que se encuentra en el servidor. Las banderas que contiene este comando son: –c que indica la ruta donde está el archivo de configuración de barnyard2.conf, -d hace referencia a la carpeta donde se encuentran los log de Snort, con la bandera -f indica donde está el archivo .u2, -w da la localización del archivo Waldo y –u hace referencia tanto al grupo como al usuario Snort. En la Figura 44 se puede ver los eventos que se generan con el comando que se detalló en el punto anterior.

Generación de los eventos detectados por Snort

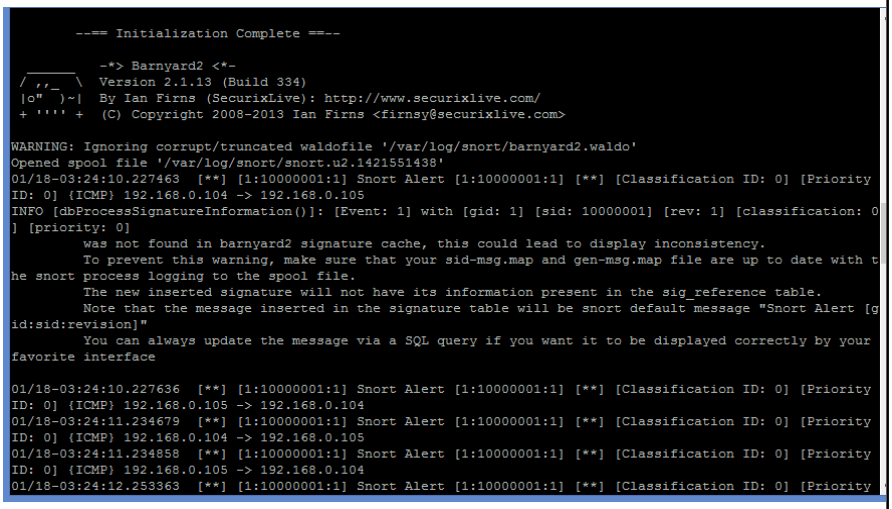


Figura 44. Generación de los Eventos

Elaborado por: Santiago Acosta y Jimena Muñoz

- Ahora verificar en la base de datos Mysql si los eventos de barnyard se escribieron. Correr el siguiente comando en la consulta de mysql.

  - *mysql –u Snort –p –D Snort –e "select count(*) from event"*

3.16 Snorby

Snorby es una aplicación web front-end, escrita en Ruby, para aplicaciones que registre eventos de formato binario u2. Snorby se integra con un sistema de detección de intrusos como puede ser Snort, Suricata y Sagan; en este caso se tomará a Snort como motor de

IDS. El objetivo principal de este aplicativo es que sea altamente competitivo con código abierto y libre para el monitoreo de redes, ya sea para uso privado home o empresarial de alto nivel. (López, 2014, pág. 39).

3.16.1 Características de Snorby

En este punto se menciona algunas características importantes que nos brinda Snorby como interfaz gráfica para representar los datos obtenidos con Snort:

- Reporta los datos como comparaciones de las actividades de los sensores y de las firmas que se han utilizado para enlistar alertas de tráfico en periodos de tiempos diarios, semanales, mensuales o mensuales, estos reportes se pueden exportar en archivos PDF.
- A diferencia de otras interfaces Snorby posee un completo análisis de paquetes y sesión de datos.
- Muestra de manera más rápida las alertas generadas por los sensores.
- La plataforma de Snorby es de código abierto que está disponible en la versión 3 de la licencia permisiva de GNU.

3.16.2 Entorno de Snorby

El entorno de Snorby es muy amigable para el usuario ya que despliega gráficamente los eventos generados después de haber sensado cierto tráfico de red que haya capturado Snort.

En la Figura 45 se puede ver el acceso a la interfaz de Snorby, hay que tener en cuenta que la dirección de ingreso seria https://localhost:444, o se puede reemplazar localhost por la ip del servidor donde se encuentre montada la interfaz, al iniciar la sesión de Snorby pide mail y password que se ingresó al configurar Snorby.

Login de Snorby

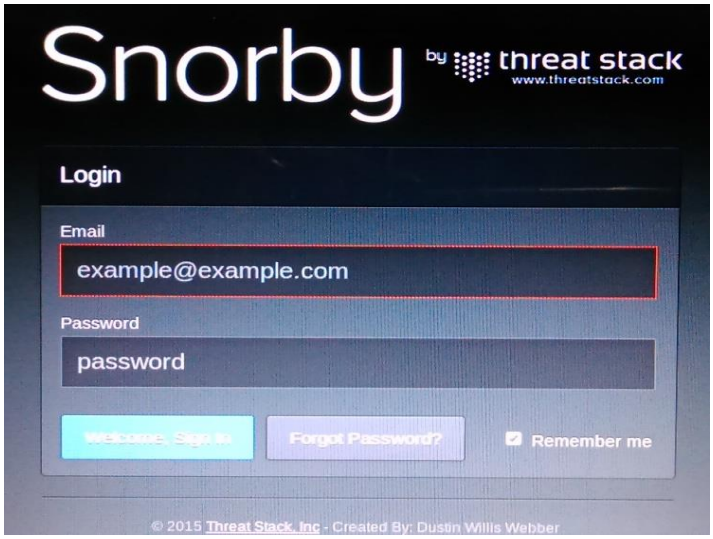


Figura 45. Interfaz de Snorby

Elaborado por: Santiago Acosta y Jimena Muñoz

Una vez dentro de la interfaz Snorby presenta algunas funciones como son:

- ***Dashboard***: que puede presentar reportes como: número de eventos, conteo de eventos vs tiempo de sensor, conteo de protocolos vs tiempo, gráficas de distribución de firmas, gráficas de distribución de fuentes de origen y destino. Aquí se puede ver como se presentan las alertas clasificándose en High Severities, Medium Severities y Low Severities.
- ***My queue***: se puede tener eventos de distribución para un mejor análisis de los eventos o alertas detectadas.
- ***Events***: Presenta una línea de tiempo de eventos con detalles incluye funciones de OpenFPC (trata de una serie de herramientas de captura de archivos de formato .pcap).
- ***Sensors***: contiene los sensores que se conectan para futuros análisis.
- ***Search***: permite filtrar eventos por criterio de análisis.
- ***Administration***: se puede encontrar varios aplicativos de control de la interfaz. (López, 2014, pág. 60).

En la Figura 46, se puede ver de mejor manera lo explicado anteriormente en cuanto a lo que se refiere a la descripción del contenido de la interfaz de Snorby.

Interfaz de Snorby

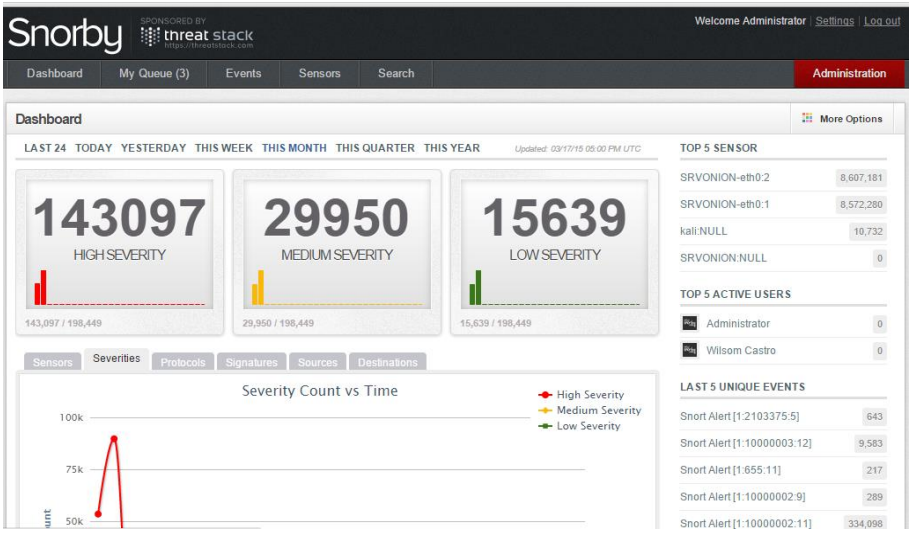


Figura 46. Descripción de Interfaz de Snorby

Elaborado por: Santiago Acosta y Jimena Muñoz

3.17 Actualización automática de las reglas de Snort

Al igual que sucede con cualquier herramienta de detección de intrusos o amenazas, es necesario tener actualizada las reglas para la detección de ataques nuevos. Para la actualización de dichas reglas con Pulledpork se procederá a inscribirse en la página oficial de Snort www.snort.org y usar el *Oinkcode* que se deberá añadir en el archivo de configuración de pulledpork.conf.

Pulledpork procesa las reglas binarias y organiza los elementos en los archivos adecuados, el paquete *Pulledpork* que va a contener el *oinkcode* viene ya incluido en sistemas operativos con distribución Debian, en Security Onion ya viene por defecto instalado. Pulledpork puede modificar las reglas durante la instalación.

- Para obtener el Oinkcode se debe ingresar a la página oficial de Snort, ir a rules y elegir Oinkcode para generar el código, como se muestra en la Figura 47.

Página del Oinkcode

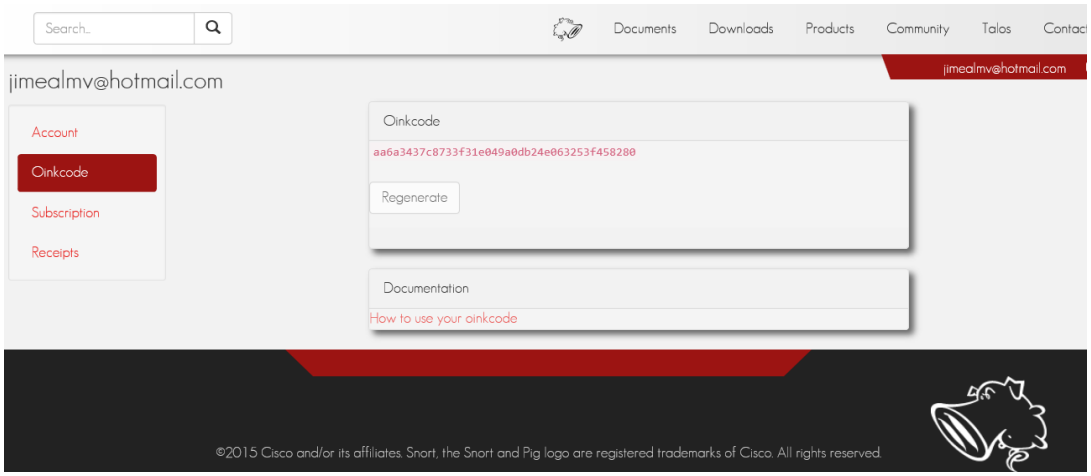


Figura 47. Generación del Oinkcode
Elaborado por: Santiago Acosta y Jimena Muñoz

Una vez obtenido el código se reemplaza en el archivo pulledpork.conf, para posteriormente ejecutar la actualización con el siguiente comando:

pulledpork.pl –c /etc/nsm/pulledpork/pulledpork.conf.

En la Figura 48 se especifica la línea en la cual debe ser modificado el oinkcode para que al ejecutar el Pulledpork proceda con la actualización de las reglas de Snort.

Configuración del código del OinkCode

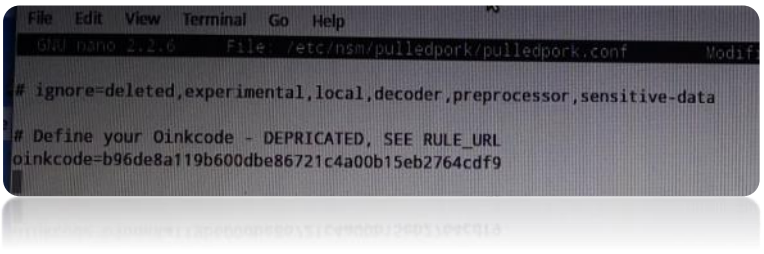


Figura 48. Configuración del Oinkcode
Elaborado por: Santiago Acosta y Jimena Muñoz

Cabe recalcar que en el planteamiento del objetivo de generar un script para la actualización automática de las reglas de Snort no se va usar ya que se usará el pulledpork que viene pre-instalado en Snorby y con la ayuda de un oinkcode se conecta a la página

oficial de Snort y así actualizará las reglas, de esta manera se cumple con el objetivo planteado, se procedió hacerlo de esta forma ya que se optimiza recursos en el procesamiento del script y hace la misma función que un script generado.

3.18 Implementación del DIDS

Para la implementación del DIDS se realizó un análisis previo de la ubicación de los dispositivos, se especificó los enlaces principales en los cuales se van a instalar las Sondas Pi, para futuros análisis. Como parte de la implementación tendremos los siguientes dispositivos:

- Servidor DIDS
- Sonda Pi 1
- Sonda Pi 2

3.18.1 Implementación del servidor DIDS

Para esta implementación primero se debe tomar en cuenta las especificaciones técnicas que debería tener el servidor, en este caso se tiene las siguientes características, en la Tabla 21 se puede ver las características del servidor DIDS:

Tabla 21. *Características del servidor DIDS*

Servidor DIDS	Características
Hardware	RAM: 8Gb HD: 2Tb Interfaces: 2 interfaces, eth0:1 y eth0:2
Software	Sistema Operativo: Security Onion (distribución Xubuntu)

Nota. Características específicas del servidor DIDS

Elaborado por: Santiago Acosta y Jimena Muñoz

El servidor está ubicado físicamente en el Data Center del edificio matriz de la EEQ, conectado en el enlace denominado de Administración, en la siguiente tabla se especifica el direccionamiento del servidor con la Vlan a la que pertenece, en la Tabla 22 se especifica el direccionamiento del servidor DIDS.

Tabla 22. *Direccionamiento del servidor DIDS*

Servidor DIDS	
Vlan	**Direccionamiento**
2	172.17.224.44

Nota. Se detalla el direccionamiento y ubicación lógica del servidor DIDS

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 49 se aprecia la implementación del servidor DIDS en el data center, no se puede mostrar más imágenes por motivos de seguridad de la Institución antes mencionada, por ende solo se puede mostrar esta imagen del servidor en el Data Center.

Servidor DIDS

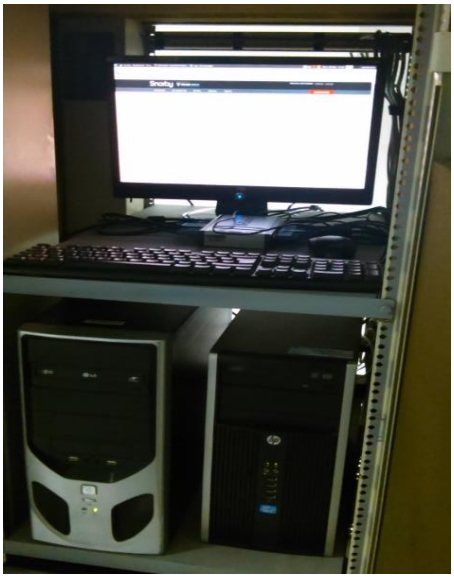


Figura 49. Implementación del servidor DIDS

Elaborado por: Santiago Acosta y Jimena Muñoz

3.18.2 Implementación de la Sonda Pi 1

Las Sondas Pi también tienen su punto específico de ubicación para sensar los puntos más críticos de la red del edificio matriz de la EEQ, en la siguiente tabla se mencionara las especificaciones técnicas, cabe recalcar que tanto esta Sonda Pi 1 como la Sonda Pi 2

tendrán las mismas características, en la Tabla 23 están las especificaciones técnicas de la sonda Pi.

Tabla 23. *Especificaciones técnicas de Sonda Pi*

Sonda Pi	Características
Hardware	RAM: 512 Mb Almacenamiento: se usa tarjetas SD de 16Gb Interfaz: 1 interfaz de red eth0

Nota. Se detalla las características en cuanto a hardware y software de la Sonda Pi

Elaborado por: Santiago Acosta y Jimena Muñoz

La Sonda Pi 1 físicamente se encuentra conectada en un switch de distribución el cual permitió el acceso al enlace del Wireless Controler, el cual se especificó anteriormente en el análisis de ubicación, en la Tabla 24 se describe el direccionamiento de la misma.

Tabla 24. *Direccionamiento de la Sonda Pi 1*

Sonda Pi 1	
Vlan	**Direccionamiento**
13	172.16.102.60

Nota. Se detalla el direccionamiento específico de la Sonda Pi 1

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 50 se muestra la ubicación de la Sonda Pi 1 físicamente en el switch de distribución que se conectó para el posterior análisis.

Sonda Pi 1

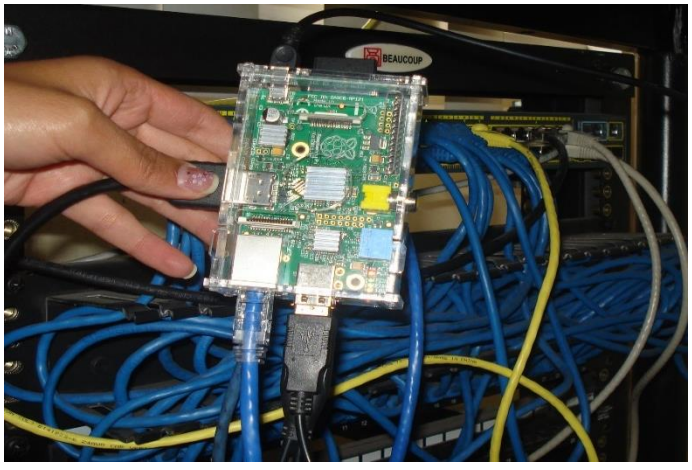


Figura 50. Ubicación física de Sonda Pi 1

Elaborado por: Santiago Acosta y Jimena Muñoz

3.18.3 Implementación de la Sonda Pi 2

La Sonda Pi 2 físicamente se encuentra conectada un punto de red que tiene acceso al enlace de Tesorería, el cual se especificó anteriormente en el análisis de ubicación, en la tabla 25 se describe el direccionamiento de la misma.

Tabla 25. *Direccionamiento de Sonda Pi 2*

Sonda Pi 2	
Vlan	**Direccionamiento**
32	192.168.100.201

Nota. Se detalla el direccionamiento específico de la Sonda Pi 2

Elaborado por: Santiago Acosta y Jimena Muñoz

En la Figura 51 se muestra la ubicación específica de la Sonda Pi 2 que se le designo anteriormente.

Sonda Pi 2

Figura 51. Ubicación física de la Sonda Pi 2

Elaborado por: Santiago Acosta y Jimena Muñoz

CAPÍTULO 4

PRUEBAS Y RESULTADOS DE LA IMPLEMENTACION DEL DIDS

4.1 Análisis de las pruebas de la implementación del DIDS.

Para las pruebas de funcionamiento de los DIDS en la Empresa Eléctrica de Quito, se utilizó la plataforma Snorby, como se tiene conocimiento es un front-end el cual presenta una interfaz gráfica muy interactiva para tener una visión amplia y rápida de lo que está sucediendo en la red EEQ.

A continuación se describe las imágenes que Snorby reportó.

En la pantalla principal del Snorby como se muestra en la Figura 52, se observa que son muy atrayente (grandes) los números que corresponde a los paquetes capturados de acuerdo al tipo de severidades o gravedad de la red de la EEQ, en este caso se presenta los tres tipos de gravedad que son gravedad alta, gravedad media y gravedad baja y así tener un breve análisis de cómo se encuentra la red.

Interfaz de Snorby

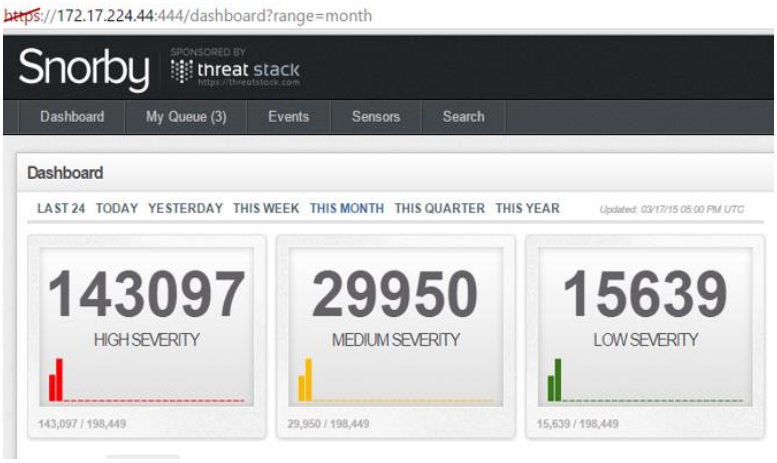


Figura 52. Pantalla principal de Snorby

Elaborado por: Santiago Acosta y Jimena Muñoz.

Si Se desea tener un mejor análisis del reporte por tiempos de este tipo de severidades, se puede escoger entre las opciones: el pasado 24 horas (last 24), hoy (today), ayer (yesterday), este mes (this month), este trimestre (this quarter) y este año (this year) y así se tendrá el reporte de acuerdo al tiempo que se vea prudente analizar los enlaces de red.

En la parte superior de la Figura 53, se observa la fecha que se realizó el reporte correspondiente al mes de marzo de 2015, de igual manera se observar los nombres de cada uno de las interfaces que están realizando la captura de los paquetes como también el número de eventos capturados, en este caso se tiene las interfaces de: administración, monitorización y el sensor Kali (sonda); las cuales reportan el siguiente análisis: eth0:1 - 100736 eventos, eth0:2 - 87913 eventos y kali - 9800 eventos y en la parte inferior de la figura en mención se presenta a través de un gráfico el cálculo de eventos vs tiempo por sensor, en este caso el tiempo del sensor corresponde a la fecha indicada anteriormente.

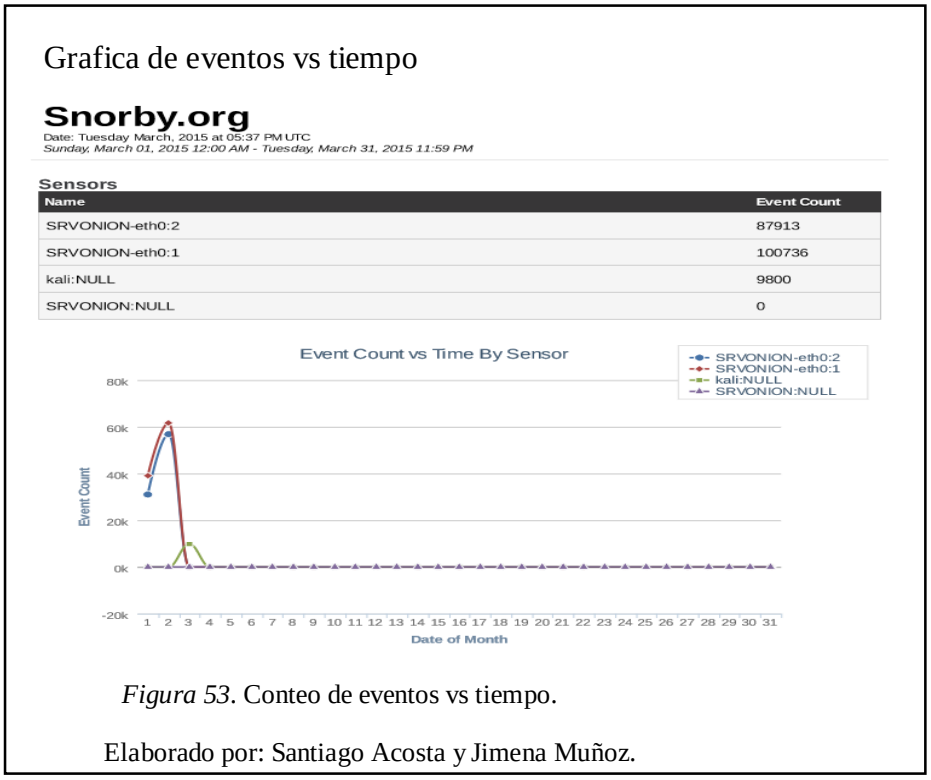


Figura 53. Conteo de eventos vs tiempo.

Elaborado por: Santiago Acosta y Jimena Muñoz.

Continuando con la descripción de la figura anterior se tiene que en la parte donde se exhibe la gráfica del conteo de eventos vs tiempo por sensor, se observa que las interfaces eth0:1 y eth0:2 el primer día inician el cálculo de eventos aproximadamente en 33kb y

39kb respectivamente y teniendo un incremento en el trascurso del siguiente día y con lo que corresponde al sensor Kali, se observa que en el trascurso del primer día el cálculo de los eventos tiene un crecimiento, llegando a un máximo 15kb.

En la Figura 54, se logra estimar en la parte superior las severidades de la red correspondiente de la Empresa Eléctrica de Quito, en donde se aprecia una gravedad alta de 143097/198449, una gravedad media de 29950/198449 y una gravedad baja de 15639/198449.

Gráfica de alertas vs tiempo

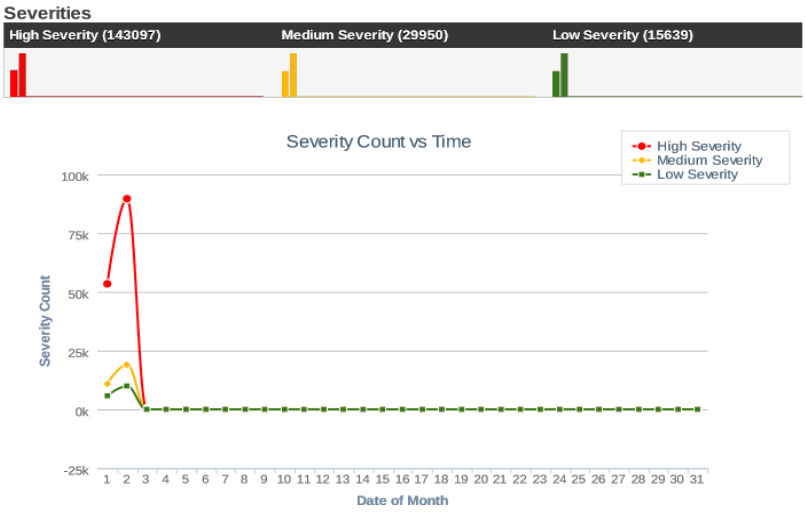


Figura 54. Conteo de alertas vs tiempo.

Elaborado por: Santiago Acosta y Jimena Muñoz.

En la gráfica de la sección del conteo de alertas vs tiempo, de la Figura 55, se observa que la gravedad alta inicia el análisis o monitorización con un cálculo de 53Kb y en el trascurso de los días subsiguientes llega a presentar un cálculo máximo aproximado de 93kb, la cual es la gravedad más alta y representa una vulnerabilidad critica; con respecto a la gravedad media se observa un incremento considerable en el trascurso de los días sucesivos reportando el cálculo máximo es de 23kb, hay que tomar muy en cuenta ya que está gravedad media puede volverse un caso grave es decir una gravedad alta y la gravedad

baja se observa que tiene un cálculo máximo aproximado del 12kb es bajo pero igual hay que tener muy en cuantas si los valores van subiendo.

En la Figura 55, se puede observar los protocolos que están siendo sensados los mismos que son: protocolo TCP 177266 eventos, protocolo UDP 15181 eventos e ICMP 6006 eventos, registrando un total de 198449 eventos.

Gráfica de protocolos vs tiempo

Protocols

TCP Count	UDP Count	ICMP Count	Total
177266	15181	6006	198449

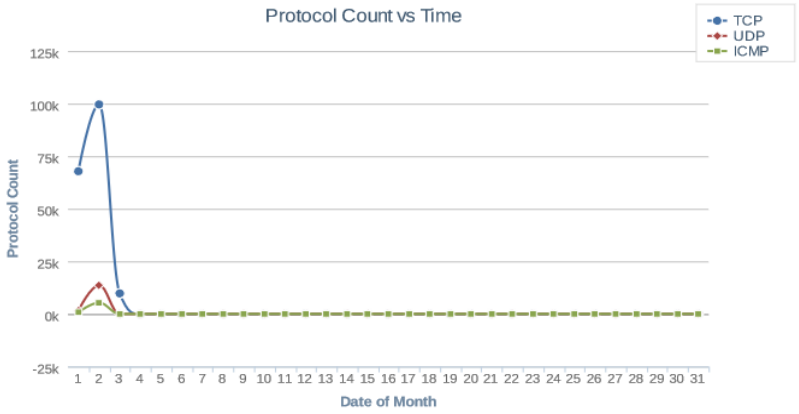


Figura 55. Conteo de protocolos vs tiempo.

Elaborado por: Santiago Acosta y Jimena Muñoz.

En ítem donde se presenta una gráfica estadística de los conteo de protocolos vs tiempo de la Figura 55, se observa que protocolo TCP inicia el análisis en 70kb y en el trascurso de los días siguientes el protocolo TCP tuvo un conteo considerable llegando a detectar 100kb, con respecto a los protocolos de UDP y ICMP se aprecia que el registro de los dos protocolo inician en 0kb y en el trascurso de los días subsiguientes se incrementa llegando a detectar un máximo de 21kb y 5kb paquetes de protocolos respectivamente.

En la Figura 56, se estima una tabla donde se presenta el top 15 de las firmas o también llamadas reglas del Snorby, donde se puede distinguir el nombre, el porcentaje y el número de eventos correspondiente a cada firma.

Gráfica del top 15 de firmas de Snort

Top 15 Signatures

Signature Name	Percentage	Event Count
ET POLICY TeamViewer Dyngate User-Agent	47.11%	91387
ET POLICY Data POST to an image file (gif)	22.56%	43756
GPL SNMP public access udp	7.07%	13720
ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Brows...	6.19%	11999
Snort Alert [1:10000003:12]	4.94%	9583
GPL ICMP_INFO PING Cisco Type.x	3.03%	5880
ET USER_AGENTS Binget PHP Library User Agent Outbound	1.2%	2321
ET POLICY Unsupported/Fake FireFox Version 2.	1.18%	2292
ET POLICY RDP connection confirm	1.15%	2221
ET POLICY RDP connection request	1.13%	2199
ET TROJAN MS Terminal Server User A Login, possible Morto inbound	1.08%	2091
ET POLICY RDP disconnect request	0.78%	1506
ET POLICY PE EXE or DLL Windows file download	0.53%	1030
ET TFTP Outbound TFTP Read Request	0.48%	923
ET POLICY SSLv3 outbound connection from client vulnerable to ...	0.34%	667
ET POLICY GNU/Linux APT User-Agent Outbound likely related to ...	0.28%	541
ET POLICY Vulnerable Java Version 1.7.x Detected	0.28%	539
ET INFO Packed Executable Download	0.27%	529
GPL SQL service_name buffer overflow attempt	0.2%	395
ET POLICY Dropbox.com Offsite File Backup in Use	0.2%	388

Figura 56. Top 15 de firmas
Elaborado por: Santiago Acosta y Jimena Muñoz.

En el mes de marzo de 2015 se realizó el proceso de monitorización del tráfico de información correspondiente al segmento de la red del edificio matriz de la EEQ, buscando patrones de ataques en los puntos críticos de la red, dicha monitorización se lleva a cabo desde las sondas Rasberry Pi y también de la interface de monitorización conectadas a la red interna de la EEQ, donde se realizó un barrido de dicha red, las Sondas luego de realizar dicho análisis, informó a una estación administrativa centralizada en este caso es un servidor con el sistema operativo Segurity Onion el cual tendrá previamente instalado el Snorby, donde se tendrá la base de datos de las firmas y ataques conocidos.

Para tener una mejor perspectiva de las firmas o reglas, la Figura 57, muestra un pastel estadístico, donde la firma con mayor porcentaje que se registro fue: ET POLICY TeamViewer Dyngate User-Agent (47.11% - 91387 eventos) y concurrió de tipo TCP la misma que se detalla en la Figura 56, de igual manera hay que tomar en consideración que existe una alerta de tipo ***Troyano*** de nombre “ET TROJAN MS Terminal Server User A

Login, possible Morto inbound" con un porcentaje del 1%, registrando o detectando un total de 2091 de eventos.

Gráfica de estadísticas del top 15 de las firmas de Snort

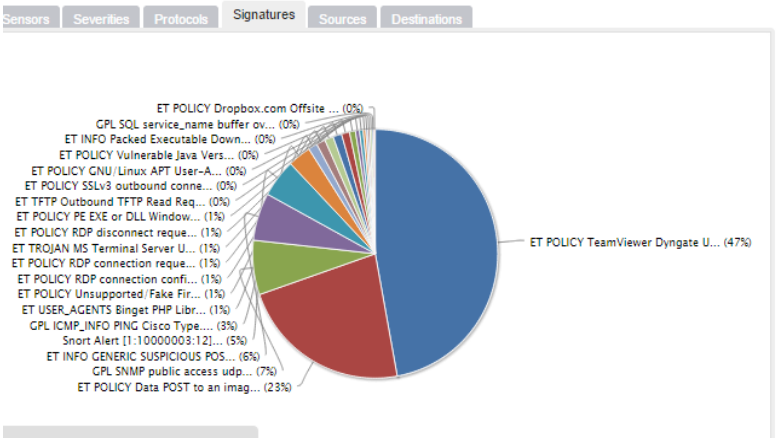


Figura 57. Pastel estadístico del top 15 de las firmas.

Elaborado por: Santiago Acosta y Jimena Muñoz.

A continuación Figura 58 se observa la Información de la regla ET POLICY TeamViewer Dyngate User-Agent.

Contenido de una regla de Snort registrada por Snorby

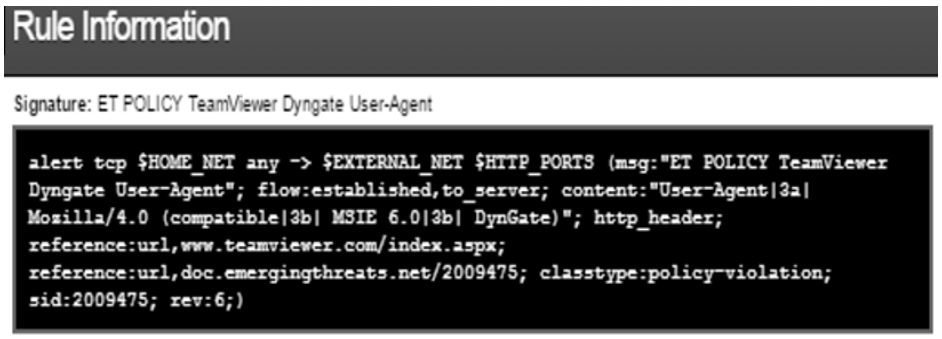


Figura 58. Información de la regla ET POLICY TeamViewer Dyngate User-Agent.

Elaborado por: Santiago Acosta y Jimena Muñoz.

Se analizó que dicha firma tiene una acción de tipo "alerta", con dicha acción se podrá establecer que se debe hacer sobre dichos paquetes, el protocolo de comunicación que este

tráfico utilizo es TCP, proviene de la red de origen censada la misma que estará definida por la variable $HOME_NET en este caso corresponderá a la red de la Empresa Eléctrica Quito, con el uso de la palabra "any" se llena los campos de los puerto de comunicación de origen para tener un amplio análisis de la red, a la dirección y/o sentido de comunicación estará establecida por el símbolo "->" en este caso será hacia la red de destino, la cual será establecida por la variable $EXTERNAL_NET lo que permitirá analizar hacia una red externa de la empresa.

Los puertos de destino de igual manera quedará establecida por la variable $HTTP_PORTS, dentro del paréntesis se encuentran las opciones de las reglas las cuales están separadas entre sí, por (;) y las claves de las opciones están separadas por (:) en dicha regla podemos visualizar las siguientes opciones "msg" donde informa al motor de la alerta que mensaje debe mostrar; "flow" se usa para indicar que regla se debe aplicar solo en ciertos tipos de tráfico en este caso solo se usa con el flujo de TCP; "content" es una búsqueda sensitiva para un conteo específico del tráfico del payload del paquete; "reference" detalla un enlace a sistemas de identificación de ataques externos; "classtype" puntea qué tipo de ataques intentó el paquete, dicha opción usa las classification las cuales se encuentran definidas en archivos como classification.config del Snort ; "sid" en conjunto con "rev" identifica una regla del Snort, correlacionando el ID de la regla individual con la revisión de la regla. (González Gómez, 2003, pág. 65)

El la Figura 59 se puede observar el evento fuente correspondiente a la interfaz de monitorización eth0:2, donde en las columnas se muestran distintos tipo de gravedad (alta: color rojo, media: color amarillo y baja: color verde), el nombre del sensor que lo detecto en este caso es la interfaz eth0:2, IP's de origen puede ser una dirección IP de la red de la Empresa Eléctrica o una dirección IP externa, IP de destino de una red externa o dirección IP de la red de la Empresa Eléctrica , firma del evento donde muestra el mensaje de la regla, marca de tiempo lo que representa la fecha que fue censada.

Eventos de la interfaz de monitoreo eth0:2

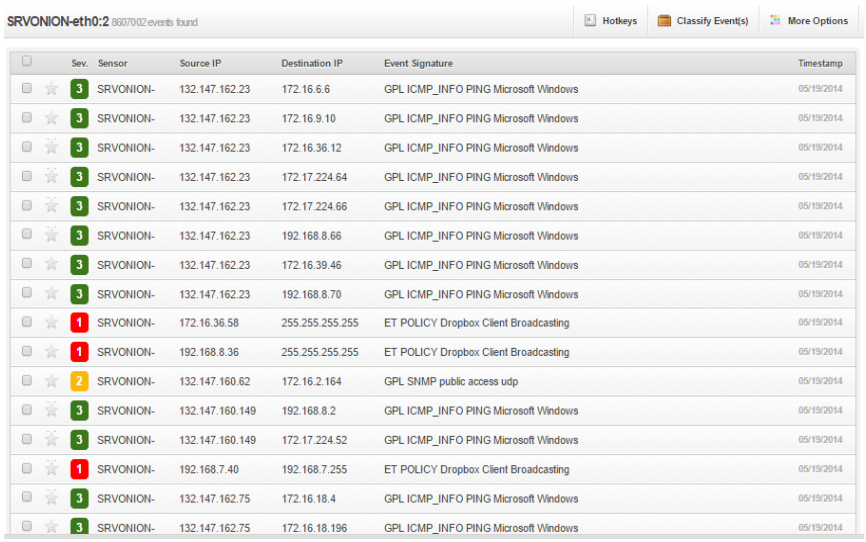


Figura 59. Evento fuente de la interfaz de monitoreo eth0:2.

Elaborado por: Santiago Acosta y Jimena Muñoz.

En el evento fuente de la interfaz de monitorización etch0:2, se observa que la regla GPL ICMP_INFO PING Microsoft Windows y es una alerta de gravedad baja, la cual se observa más detalladamente en la Figura 60.

Regla de Snort GPL ICMP_INFO PING Microsoft Windows

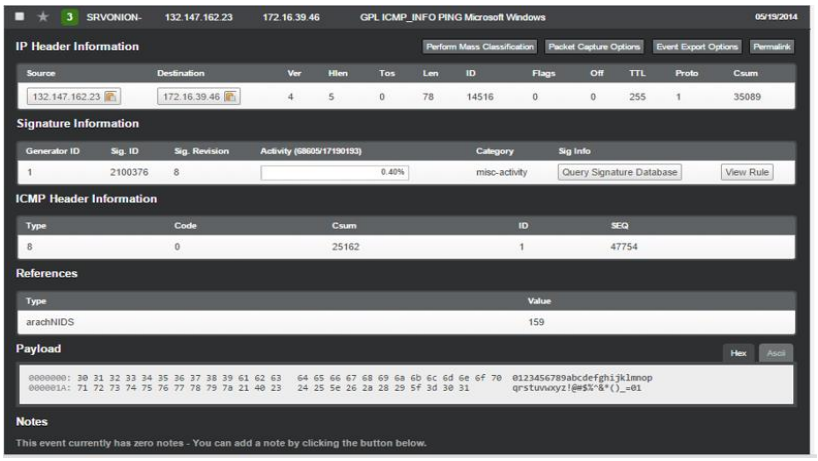


Figura 60. Regla GPL ICMP_INFO PING Microsoft Windows.

Elaborado por: Santiago Acosta y Jimena Muñoz.

Al momento de hacer clic en un evento detectado de la lista de eventos, como se muestra en la Figura 59, se expandirá una nueva pantalla que se muestra en la Figura 60 donde se revela una información de la regla que anteriormente fue mencionada, donde se puede observar la información del encabezado IP, información de la firma o regla detalla, información del encabezado ICMP, referencias y el contenido de la carga útil "Payload" en hexadecimal o ASCII.

En la Figura 61 se ve detalladamente la regla GPL ICMP_INFO PING Microsoft Windows, la que es de tipo ICMP.

Captura de regla de Snort GPL ICMP_INFO PING Microsoft Windows

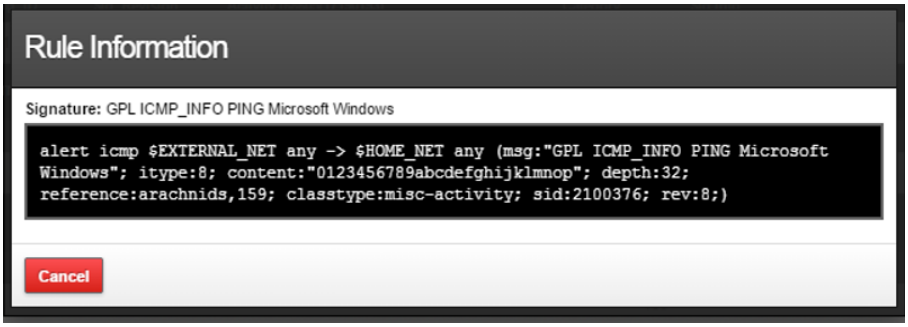


Figura 61. Información de la regla GPL ICMP_INFO PING Microsoft Windows

Elaborado por: Santiago Acosta y Jimena Muñoz.

La siguiente regla como se evidencia en la Figura 62, posee la acción de tipo "alerta", la cual indicará que hacer con el paquete analizado o censado, el protocolo que fue analizado en la regla es ICMP, la red de origen estará establecida por la variable $EXTERNAL_NET en este caso será una dirección IP externa (132.147.162.23).

La red de destino está establecida por la palabra cualquier "any" permitirá tener un gran amplio análisis de la red, la dirección de comunicación estará establecida por el símbolo "->" donde se observa que está dirigida hacia la variable $HOME_NET lo cual será nuestra red interna de la empresa eléctrica (172.16.39.46), los puertos de destino estarán determinado por la palabra "any" lo que se entiende es que serán analizados todos los

puertos, dentro de los paréntesis se encuentran las opciones de las reglas como “msg” es el mensaje que se mostrara de la regla, “content” realizara un conteo especifico del tráfico del Payload, “reference” corresponde al enlace hacia el sistemas de identificación de ataques externos; “classtype” indica qué tipo de ataques intentó el paquete, “sid” en combinación de “rev” identifica una regla especifica del Snort.

El evento fuente del sensor Kali (sonda pi); tal como se muestra en la Figura 62, donde se presentan los distintos tipos de gravedades (alta, media y baja), el nombre del sensor Kali (sonda pi), IP de origen, IP de destino, firma del evento, marca de tiempo.

Eventos del sensor Kali o Sonda pi

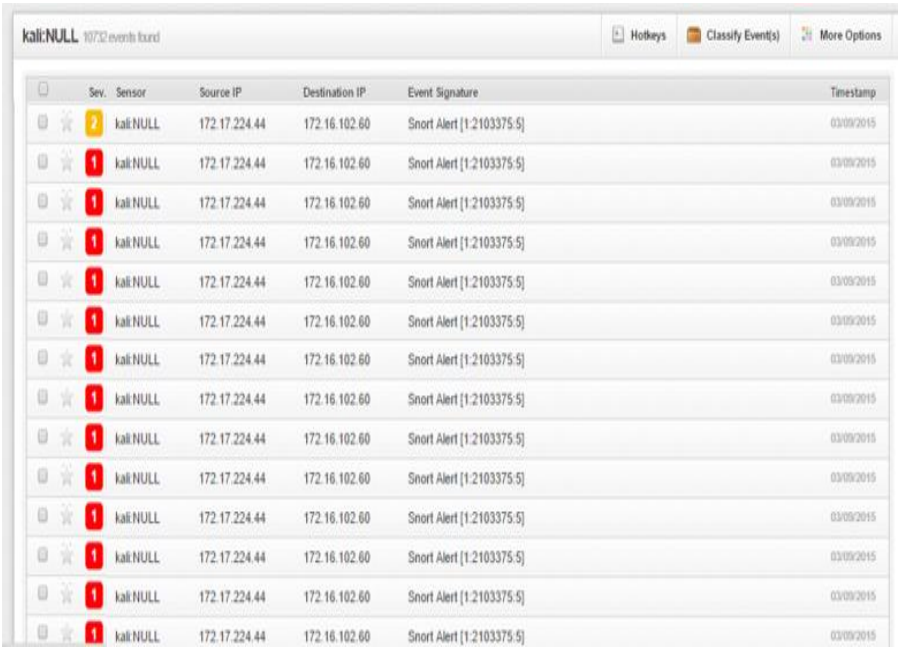


Figura 62. Evento fuente del sensor Kali (sonda).

Elaborado por: Santiago Acosta y Jimena Muñoz.

Para tener un mejor análisis vamos a dar clic en un evento de gravedad media detectado de la lista de eventos, como se muestra en la Figura 63 dicho evento contiene la regla Snort Alert [1:21103375:5], la misma que fue creada.

Regla de Snort

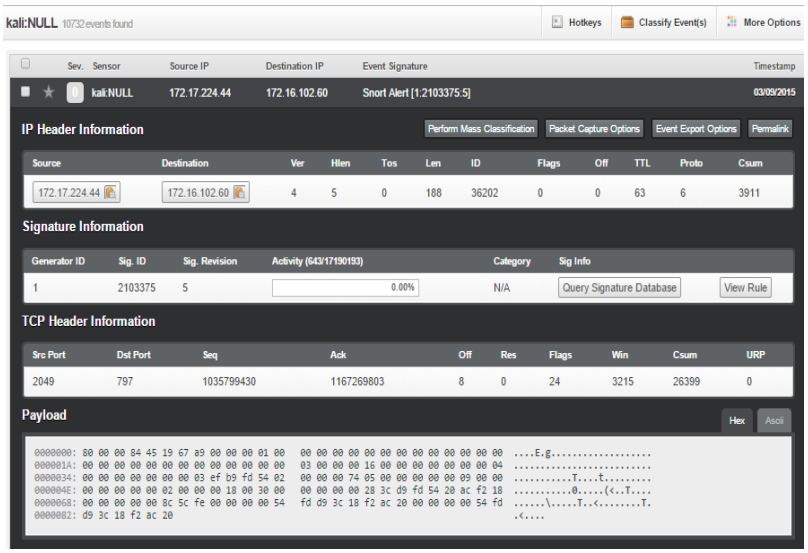


Figura 63. Regla Snort alert [1:21103375:5]

Elaborado por: Santiago Acosta y Jimena Muñoz

Luego de dar clic en la regla, se presentara una nueva ventana Figura 64, en la que se puede observar información del encabezado IP, información de la firma o regla, Información del encabezado TCP, Referencias y el contenido de la carga útil "Payload" en hexadecimal o ASCII. Dicha información presentada en la figura en mención puede ser exportada en archivo XML o enviarse a un correo electrónico.

Constructos de captura de paquetes de Snorby

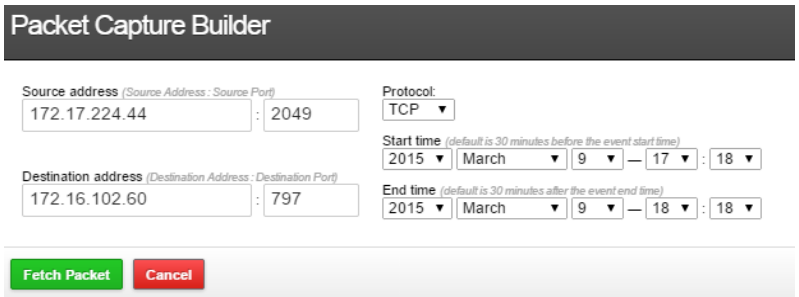


Figura 64. Constructor de captura de paquetes

Elaborado por: Santiago Acosta y Jimena Muñoz

En el constructor de captura de paquetes de la Figura 65, se puede estimar la dirección de origen que es 172.17.224.44, a través del puerto de origen 2049 (nfs sistema de archivos de red) alcanzando la dirección de destino que es 172.16.102.60 por el puerto 797 (kerberos-adm administración de base de datos Kerberos versión 5 (v5) 'kadmin', Kerberos: es una arquitectura cliente-servidor que proporciona seguridad mediante la trasferencia de datos a través de la autenticación del emisor y el receptor), el protocolo analizado es TCP y también se visualiza la hora de inicio y la hora final del sondeo.

La regla Snort alert [1:21103375:5] que fue detectada a través de la sonda pi se detallada a continuación:

alert tcp any any -> any any (msg: "Regla Snort Alert [1:21103375:5]"; sid:655; rev:11;)

La regla Snort alert [1:21103375:5], posee una acción de tipo "alerta", el protocolo detectado o analizado es de tipo TCP, con la palabra "any" se estará definiendo que sea cualquier red de origen, por cualquier puerto de origen, con el destino de comunicación "->" direccionado o establecido hacia cualquier red de destino, cualquier puerto de destino.

Dentro del paréntesis se localizan las opciones de las reglas las mismas que estarán separadas entre sí, por (;) y las claves de las opciones están separadas por (:), en la regla creada se estableció las siguientes opciones "msg" donde será el mensaje a mostrar a través del motor de la alerta, "sid" en combinación con la opción "rev" identifica una regla del Snort, correlacionando el ID de la regla individual con la revisión de la regla.

El top 10 de direcciones de origen, se observa en la Figura 65, donde se describe la dirección de IP de origen, el porcentaje y la cantidad de eventos de cada una de las direcciones IP.

Top 10 de las direcciones de origen

Top 10 Source Addresses

Source IP Address	Percentage	Event Count
172.17.240.12	15.76%	27012
172.16.14.251	14.88%	25514
172.17.229.187	10.66%	18268
172.16.34.60	9.1%	15605
172.17.230.195	8.1%	13887
172.16.100.159	8.05%	13795
172.16.18.97	6.83%	11715
172.17.232.149	5.75%	9856
172.17.224.44	5.07%	8684
172.16.5.2	3.43%	5879

Figura 65. Top 10 direcciones IP origen

Elaborado por: Santiago Acosta y Jimena Muñoz.

La dirección IP de origen con mayor porcentaje, como se muestras en la Figura 66 es la IP 172.17.240.12, esto quiere decir que de esta dirección IP originó el 16% del tráfico, lo cual corresponde a un promedio de 27012 eventos; otra dirección IP de origen, igualmente con un gran número de eventos 25514 es la IP 172.16.14.251 registrando un promedio del 15%, entre estas dos direcciones IP se puede estimar que generan más del 30% del total de tráfico de origen.

Pastel estadístico de las direcciones ip de origen

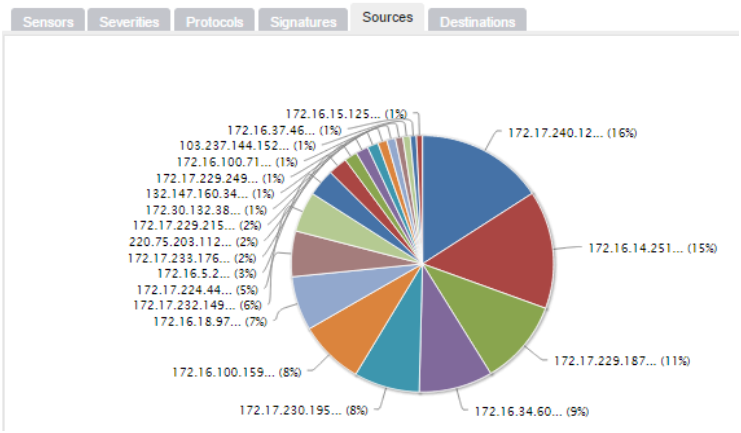


Figura 66. Pastel estadístico de las direcciones IP de origen

Elaborado por: Santiago Acosta y Jimena Muñoz.

La Figura 67, se puede evidenciar el top 10 de las direcciones IP de destino, con su porcentaje y el número de eventos de cada dirección IP.

Top 10 de las direcciones de destino de los eventos

Top 10 Destination Addresses

Destination IP Address	Percentage	Event Count
37.252.224.4	15.38%	27011
37.252.248.78	9.37%	16456
217.146.26.212	8.9%	15628
54.169.96.137	8.89%	15617
54.169.110.149	8.72%	15327
37.252.230.28	8.58%	15078
37.252.227.51	8.36%	14686
54.169.49.176	7.29%	12811
172.16.102.60	5.56%	9764
10.21.87.2	3.35%	5880

Figura 67. Direcciones IP de destino.
Elaborado por: Santiago Acosta y Jimena Muñoz.

En la Figura 68, se puede apreciar que la dirección IP con mayor destino corresponde a la IP 37.252.224.4 registrando un total de 27011 eventos, lo cual ha generado el 15 % del tráfico, adicionalmente hay que considerar que otras direcciones IP's de destino son: 37.252.248.78 - 217.146.26.212 – 54.169.96.137 – 54.169.110.149 y 37.252.230.28 y registran un porcentaje del 9 %, sumado todas las direcciones antes mencionadas logramos tener más del 55 % del total del tráfico.

Cuadro estadístico de direcciones ip de destino

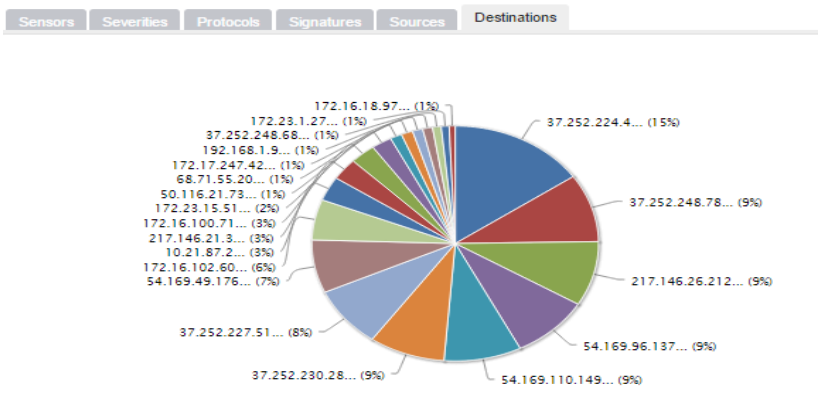


Figura 68. Pastel de direcciones IP de destino.

Elaborado por: Santiago Acosta y Jimena Muñoz.

4.2 Resultados de la implementación del DIDS

A continuación se representa las diferentes figuras comparativas entre el análisis inicial que fue expuesto en el capítulo 2 y el análisis final.

En la Figura 69, se visualiza las diferentes interfaces que fueron utilizados en el análisis inicia y análisis final, donde brevemente se acentúa, que con la Sonda Rasberry PI y el servidor Security Onion se descubre más eventos detectados por cada interfaz.

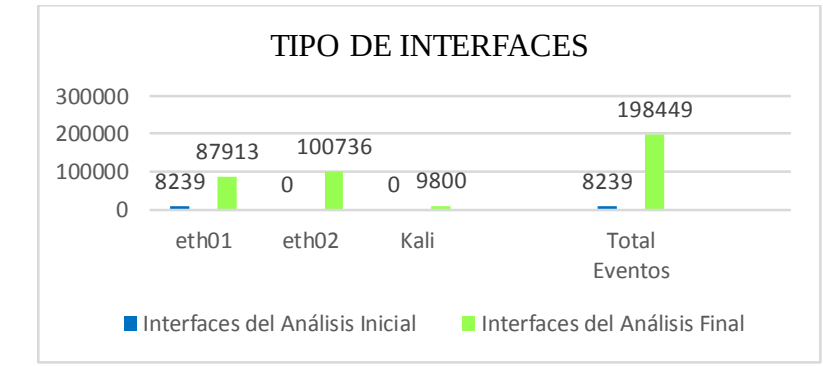


Figura 69. Interfaces de análisis inicial y final
Elaborado por: Santiago Acosta y Jimena Muñoz.

Las alertas del análisis inicial y final, que se manifiestan en la Figura 70, se puede estimar que con la ayuda de la Sonda Rasberry Pi, se obtuvo una gran cantidad de alertas altas, es decir que la seguridad de la red de la Empresa Electica de Quito tendrá mayor protección de los intrusos.

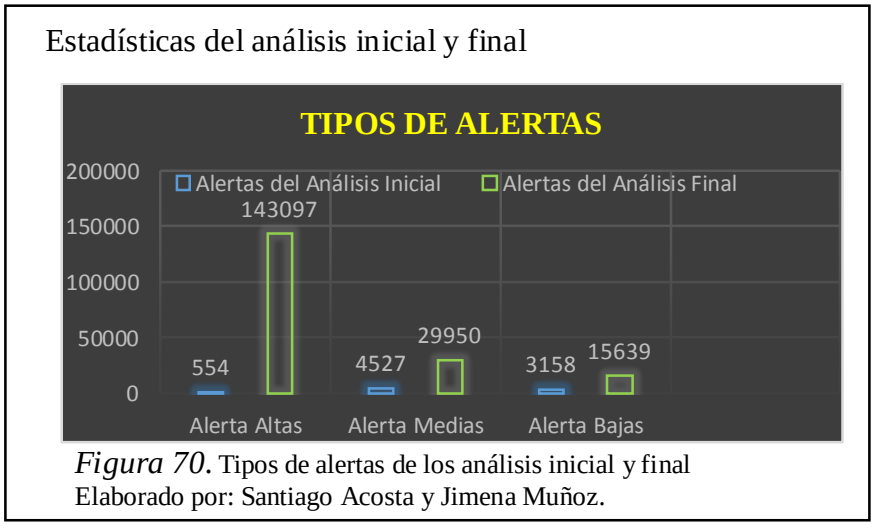


Figura 70. Tipos de alertas de los análisis inicial y final
Elaborado por: Santiago Acosta y Jimena Muñoz.

En la Figura 71, se evaluó el número por protocolo (TCP, UDP, ICMP) que fue analizado por cada tipo de Análisis en este caso el inicial y el final, registrando una mayor cantidad de protocolos detectados en el análisis final.

Estadísticas de los protocolos del análisis inicial y final

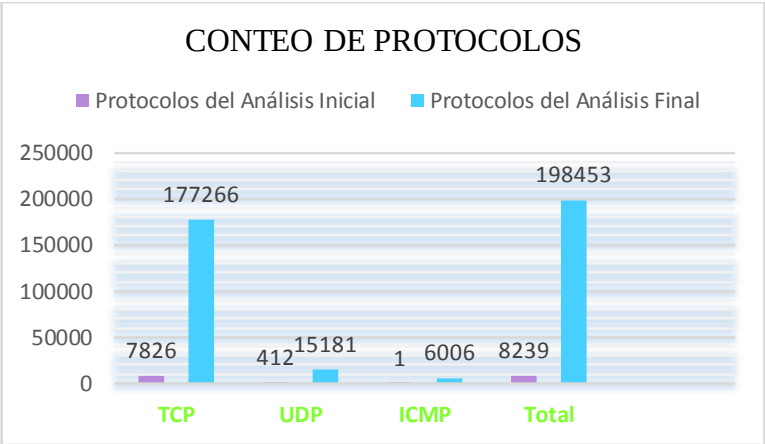


Figura 71. Protocolos del análisis inicial y final.
Elaborado por: Santiago Acosta y Jimena Muñoz.

En la Figura 72, se observa las principales firmar o reglas detectados por cada uno de los Análisis (Inicial y Final), donde se logra dar cuenta que no son las mismas reglas descubiertas, pero con el análisis inicial se tiene un registro alto por cada firma.

Estadísticas de las principales firmas detectadas

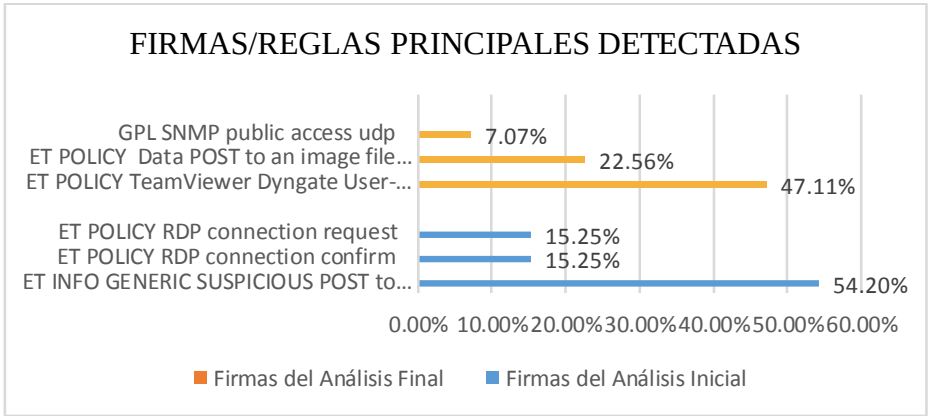


Figura 72. Firmas o Reglas del análisis inicial y final.

Elaborado por: Santiago Acosta y Jimena Muñoz.

Las Direcciones IP de origen correspondientes al análisis inicial y final, de la Figura 73, muestra que el análisis final, tiene una mejor atención por cada dirección IP y no como en el análisis Inicial, que casi una dirección IP posee más de la mitad del total de los análisis detectados.

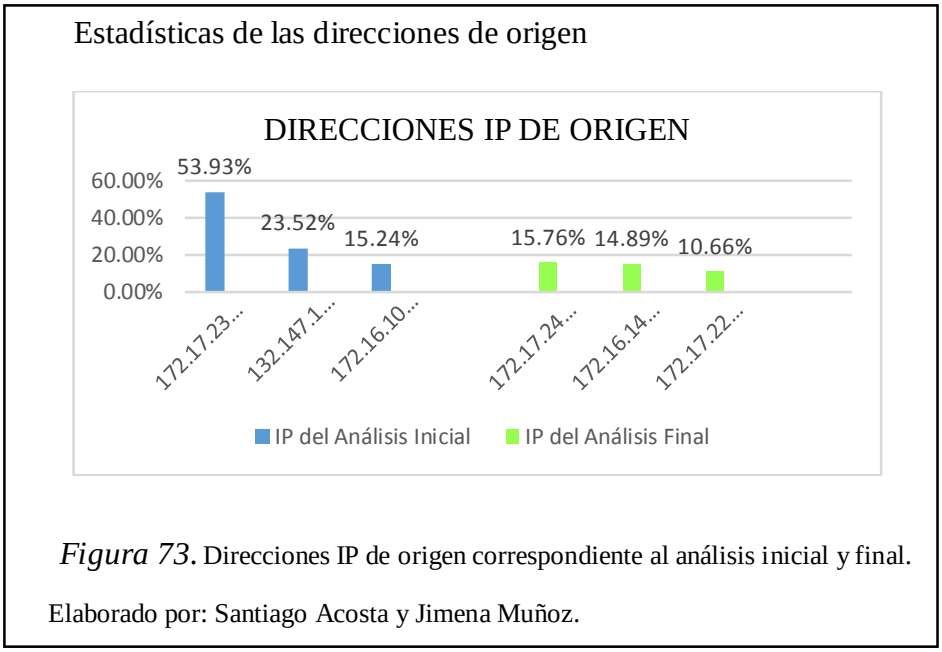


Figura 73. Direcciones IP de origen correspondiente al análisis inicial y final.

Elaborado por: Santiago Acosta y Jimena Muñoz.

En la Figura 74, se muestra las direcciones IP de destino, del análisis inicial y final, donde el análisis final modela un gran control por cada dirección de IP de destino.

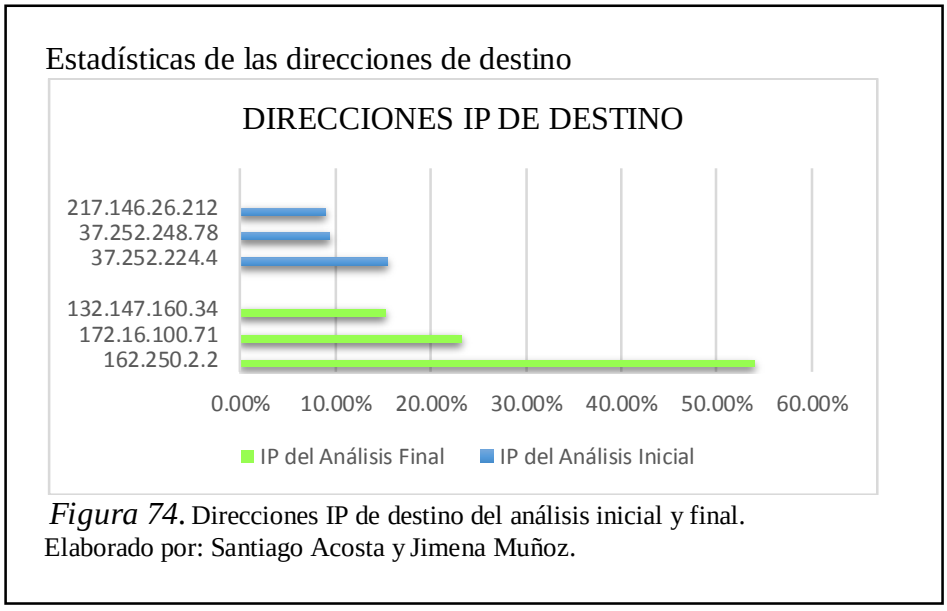


Figura 74. Direcciones IP de destino del análisis inicial y final.

Elaborado por: Santiago Acosta y Jimena Muñoz.

CONCLUSIONES

- En este proyecto se trató de mostrar la importancia de la seguridad de red y la protección de intrusiones en los sistemas de redes, con un análisis previo de la situación inicial de la red del edificio matriz de la Empresa Eléctrica Quito se realizó la implementación de un DIDS en el cual se obtuvo información de las anomalías más frecuentes en la red y así determinar cuáles son los enlaces más expuestos a intrusiones, estas anomalías se analizaron para poder generar nuevas reglas o reutilizar las reglas de Snort para obtener mejores resultados en cuanto a la detección de comportamientos anómalos y de esta manera poder mitigar de mejor manera los problemas de seguridad de la red.

- En cuanto a lo que se refiere a la implementación de un DIDS se puede decir que es un sistema que ayuda a optimizar la seguridad de una red ya que al tener sensores distribuidos por toda la red permite tener un campo más amplio de monitorización y evitar enlaces aislados, al igual que permite producir una única respuesta a intrusiones detectadas desde varios puntos de la red, y así poder establecer una solución efectiva. Entre los beneficios que proporciona este sistema es el reducir el consumo de recursos de hardware y software ya que es un sistema dividido en partes incluso la capacidad de procesamiento de detección de alertas y tiempos de respuesta es mucho más rápido que un sistema centralizado. Cabe recalcar que el mayor beneficio es el ahorro de recursos económicos debido a que se usa software libre con alto nivel de rendimiento, sin necesidad de obtener licencias por el uso de los programas que permiten hacer posible el funcionamiento de este sistema.

- En el procedimiento del uso de las reglas para mejorar la detección de anomalías se puede constatar que es posible hacer las modificación necesarias de las reglas ya existentes para tener más control en cuanto al monitoreo y así reducir la cantidad de falsos positivos que se den durante el proceso. No hay que dejar de lado que se pueden crear reglas con mayor afinamiento para una detección rigurosa de amenazas, según lo crea necesario.

- Debido a que Security Onion es un sistema operativo muy robusto dedicado para detección de intrusiones se verifica que la actualización del set de firmas de Snort se la puede hacer mediante el Pulledpork que es un script que ya vine embebido en el sistema operativo y solo se necesita el oinkcode que es el código que permite realizar la actualización mensual del set de reglas de una forma más sencilla y segura.

- Como conclusión del desarrollo de este proyecto de titulación se puede mencionar que un DIDS es una herramienta muy poderosa de fácil acceso en cuanto a costos. La detección, prevención a futuro y precaución de posibles intrusiones en una red son las mayores ventajas que puede ofrecer dicho sistema, los más beneficiados con esta herramienta en las mejores condiciones serían los administradores de red ya que sería un plus más a la seguridad ya existente y así podrían mejor el rendimiento y QoS.

- Con los resultados obtenidos de los monitores realizados por parte de las Sondas Pi se puede concluir que la red del edificio de la Empresa Eléctrica Quito es muy vulnerable, partiendo desde el hecho que es una red que no tiene un modelo jerárquico a seguir. La herramienta que se implementó fue de gran ayuda ya que se pudieron descubrir puntos críticos de fallos y así en dicha institución puedan tomar las medidas correspondientes. Con todo esto se comprueba que el sistema es apto y es utilizable en cualquier entorno de red.

RECOMENDACIONES

- Debido a que la Red del edificio matriz de la Empresa Eléctrica Quito no se maneja con un modelo jerárquico se recomienda una reestructuración de la red ya que se pudo constatar en el Diagrama de la Topología Física del Edificio matriz de la EEQ, poseen muchas falencias.

- Para futuras implementaciones de IDS con sondas pi o Raspberry pi se recomienda usar la última versión que es la B2 ya que tiene 1 RAM de procesamiento.

- La seguridad de redes es algo muy necesario para cualquier organización por esa razón sería muy importante que las instituciones educativas se proyecte a un mayor desarrollo educativo en esta área y a su vez con la educación del cuidado de una red como usuarios finales.

LISTA DE REFERENCIAS

academia.edu. (s.f.). *ARQUITECTURA ARM*. Obtenido de http://www.academia.edu/7600362/ARQUITECTURA_ARM

Andrade, J. (11 de 08 de 2012). *engadget*. Obtenido de http://es.engadget.com/2012/08/11/raspberry-pi-model-b-analizado/

Arteaga Delgado, G., & Atiaga Galeas, P. (10 de sep de 2013). *Sistema de proteccion integral aplicable a redes de área metropolitana privadas y redes de área de campus contra ataques de Malware moderno*.

Beale, J., Baker, A., & Ester, J. (2007). *Snort IDS and IPS toolkit*. Madrid: Syngress.

Brickmanne, M. d. (s.f.). *Detector de intrusiones ligero para redes*. Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.dit.upm.es%2F~joaquin%2Flas%2Ftrabajos%2F2001%2FSNORT.pdf.gz&ei=B6WpVJPVEsaZNp6TgrAJ&usg=AFQjCNENG3TMIIRZIEK3MEpPRfy5NfyTjg&cad=rja

Caballero, A. (feb de 2015). *Penetration testing, Re-Defined A project by Offensive Security*. Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

Coll Almela, C. (Septiembre de 2001). *SIRIUS: Sistema de Detección en la Red de Intrusiones. Aplucación en la Universidad de Murcia*. Obtenido de https://www.rediris.es/cert/doc/pdf/sirius.pdf

Ellingwood, J. (30 de Abr de 2014). *How to set up an NFS mount on Ubuntu 14.04*. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-set-up-an-nfs-mount-on-ubuntu-14-04

Empresa Eléctrica Quito. (2015). *Portal de la Empresa Eléctrica Quito*. Obtenido de http://www.eeq.com.ec:8080/nosotros/estructura-organizacional

Empresa Eléctrica Quito. (2015). *Portal Empresa Electrica Quito*. Obtenido de http://www.eeq.com.ec:8080/nosotros/planificacion

Giménez, M., & Gómez, J. (2008). Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Almería, España: http://www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf.

González Gómez, D. (Julio de 2003). *Sistema de Detección de Intrusiones*. Obtenido de http://derecho-internet.org/docs/ids.pdf

IET. (2013). *youtube*. Obtenido de https://www.youtube.com/watch?v=XTmo1154FSY

Jiménez Galindo, C. (2009). *Diseño y Optimización de un Sistema de Detección de Intrusos Híbrido*. Obtenido de http://www.adminso.es/images/8/88/PFC_carlos.pdf

Linux Digest. (03 de 05 de 2014). *Configuring Snort with Barnyard2, SnortReport, Acid in Ubuntu 14.04*. Obtenido de https://sathisharthars.wordpress.com/tag/barnyard2/

López, O. (oct de 2014). *Herramientas para gestionar incidentes de seguridad de redes.* Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/5776/TESIS_Oscar2.pdf?sequence=1

Mira Alfaro, E. J. (Octubre de 2001). *Implantación d eun Sistema de Detección de Intrusos de la Universidad de Valencia*. Obtenido de http://rediris.es/cert/doc/pdf/ids-uv.pdf

Muñoz, A. C. (10 de 09 de 2014). *Acerca de la Raspberry Pi*. Obtenido de ciudadred: http://ciudad.red/blog/2014/08/acerca-de-la-raspberry-pi

Ortega, U. Z. (15 de Octubre de 2004). *Sistema de Detección de Intrusos*. Obtenido de Google Scholar: http://sites.google.com/site/edicedic/archivador/EstadoDelArteIDS.pdf

Raspberry Pi en Español. (2011). *rasberryshop*. Obtenido de http://www.raspberryshop.es/hardware-raspberry-pi.php

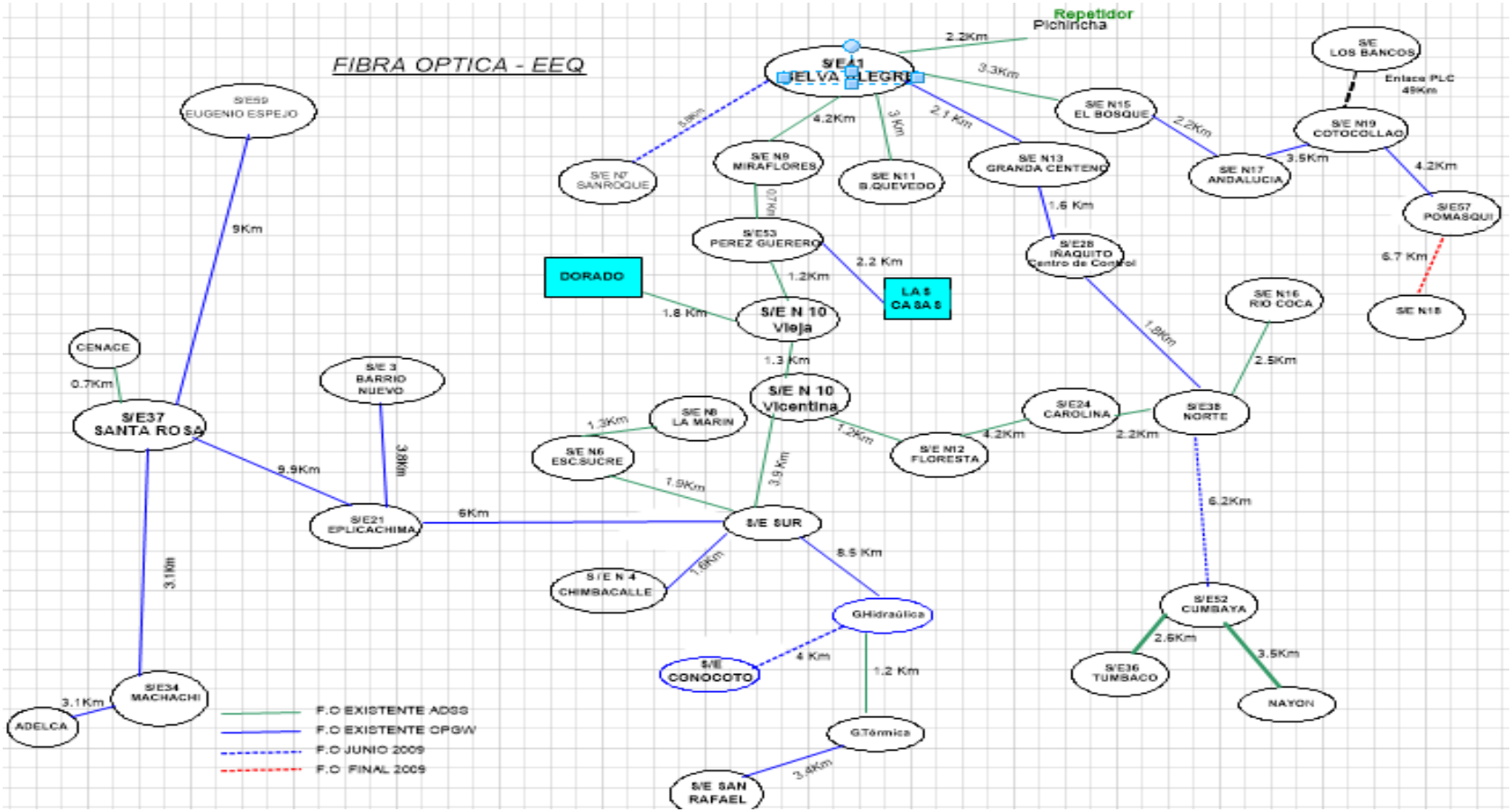
Sayago Giovanni, Tarazona Gustavo. (2014). Obtenido de https://seguridadinformaticaufps.wikispaces.com/file/view/trabajo+seguridad+(1).pdf

Security Onion. (25 de feb de 2013). *IntroductionToSecurityOnion*. Obtenido de http://code.google.com/p/security-onion/wiki/IntroductionToSecurityOnion

Torres V, D. S. (2012). Instalación, Configuración y Funcionamiento del IDS Snort. San José de Cúcuta. Obtenido de http://itfreekzone.blogspot.com/2010/08/customizando-snort.html

ANEXOS

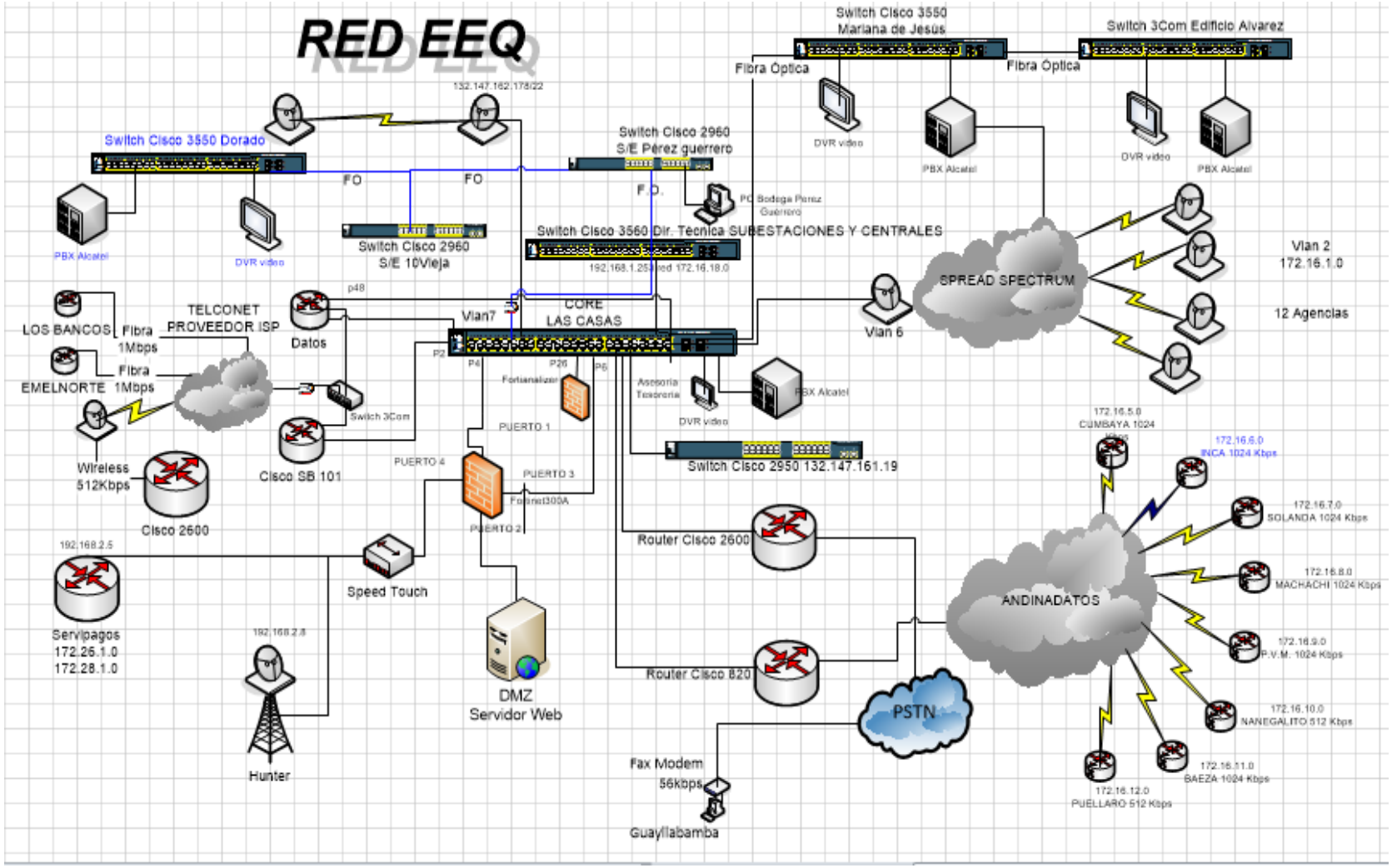
Esquema de la topologia de fibra óptica de la Empresa Electrica Quito



Anexo 1. Topología de fibra óptica

Elaborado por: Santiago Acosta y Jimena Muñoz

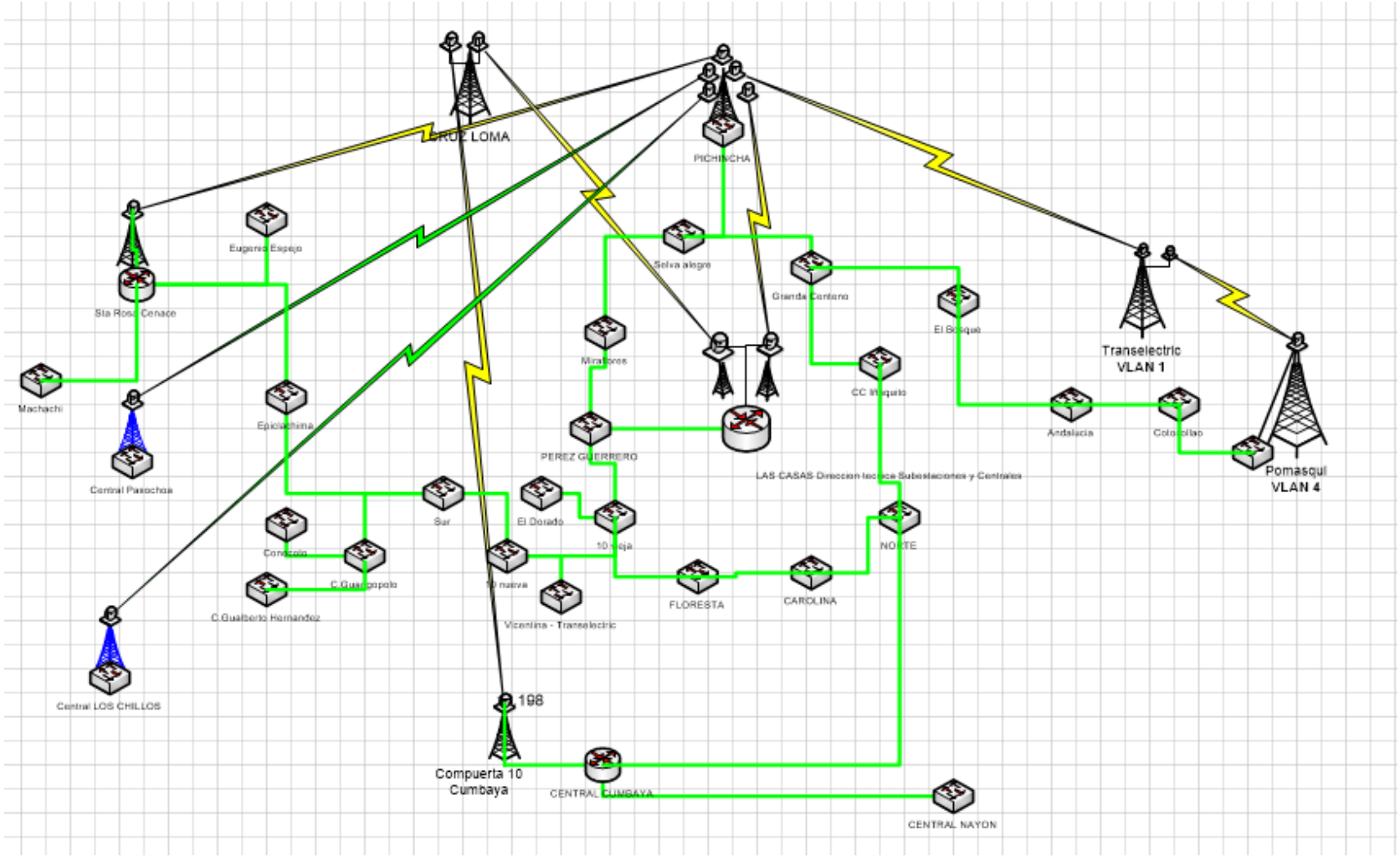
Esquema de topología de vlan’s



Anexo 2. Topología de vlan's

Elaborado por: Santiago Acosta y Jimena Muñoz

Esquema de la topología de las subestaciones y centrales de generación de la Empresa Eléctrica Quito



Anexo 3. Diagrama de red de la EEQ subestaciones y centrales de generación

Elaborado por: Santiago Acosta y Jimena Muñoz